Sécurisation de la couche physique des communications sans contact de type RFID et NFC

Pierre-Henri Thevenon

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Optique et Radiofréquence (OR)**

Arrêté ministériel : 7 août 2006

Présentée par

Pierre-Henri Thevenon

Thèse dirigée par **Smail Tedjini** et
codirigée par **Olivier Savry**

préparée au sein du **CEA-LETI**
dans **l'École Doctorale d'Electronique, Electrotechnique, Automatique & Traitement du Signal (EEATS)**

Sécurisation de la couche physique des communications sans contact de type RFID et NFC

Thèse soutenue publiquement le **10 novembre 2011**,
devant le jury composé de :

M. Gildas Avoine
Professeur, Université catholique de Louvain, Louvain-la-Neuve, Belgique, Rapporteur
M. Hervé Chabanne
Adjoint au directeur, Morpho, Issy-les-Moulineaux, Rapporteur
M. Alain Sibille
Professeur, Télécom ParisTech, Paris, Membre
M. Alain Fanet
Directeur, Tagsys RFID, La Ciotat, Membre
M. Smail Tedjini
Professeur, ESISAR, Grenoble-INP, Valence, Directeur de thèse
M. Olivier Savry
Ingénieur de recherche, CEA-LETI, Grenoble, Encadrant

Invité :
M. Francisco Marcos de Assis
Professeur, Université fédérale de Campina Grande, Campina Grande, Brésil

REMERCIEMENTS

Les travaux présentés dans ce mémoire de thèse ont été réalisés au LETI/DSIS/LCS/ANP. Je tiens donc tout d'abord à remercier Dominique Noguet, chef du groupe ANP, Laurent Hérault, chef du laboratoire LCS et Roland Blanpain, chef du département DSIS pour m'avoir permis de travailler au sein de leurs laboratoires. Un grand merci à François Vacherand pour son appui pour l'obtention de cette thèse et de son soutien pendant toute la durée de la thèse.

Je remercie Gildas Avoine et Hervé Chabanne pour avoir accepté d'être rapporteur de cette thèse. Merci également aux autres membres du Jury qui ont accepté de juger ce travail : Alain Fanet et Alain Sibille. Je vous remercie par avance des commentaires et des remarques que vous apporterez et qui me permettront de progresser et d'avoir un autre point de vue sur le travail réalisé. Merci à Francisco Marcos de Assis pour sa présence à ma soutenance de thèse en tant qu'invité.

Je tiens également à remercier Olivier Savry pour m'avoir proposé ce sujet et pour avoir co-encadré ma thèse. Merci également à Smail Tedjini pour avoir dirigé mes travaux de recherche. Merci pour tout le savoir que vous m'avez transmis. Merci pour vos conseils, pour les réponses que vous m'avez apportées et pour tout le travail de correction des articles et de ce mémoire. Merci de m'avoir transmis ce goût et cette passion pour la recherche scientifique.

J'exprime également ma profonde gratitude à tous ceux qui ont répondu présent lorsque j'en avais besoin. Je tiens à remercier particulièrement Florian Pebay-Peyroula et Jacques Reverdy pour leurs conseils et leur aide précieuse. Merci à Thierry Thomas pour ces explications complexes sur les antennes. Merci Jean-Louis Derlon pour les différents circuits électroniques réalisés. Merci à Sana Ben Hamida pour tout le travail accompli ensemble et les nombreux résultats obtenus.

Merci

A mes parents,

Difficile d'exprimer tout ce que l'on ressent quand on a eu la chance d'avoir eu pendant toutes ces années des parents qui ont sacrifié tout leur temps pour leurs enfants.
Vous êtes le meilleur exemple qu'un enfant puisse avoir.
Profitez quand même de votre vie,
Je vous dédie ce mémoire.

A Marie,

Tu es l'ainée de notre petite famille et tu en as sans aucun doute toutes les qualités. Merci pour tous les moments qu'on a passé ensemble. Je te souhaite énormément de bonheur.

A Mathieu,

Je pense que ma sœur a trouvé la personne idéale pour partager sa vie. Continue de prendre soin d'elle comme tu le fais.

A Timothée,

Tu as des parents formidables qui t'aiment énormément. Je te souhaite une vie pleine de bonheur.

A Emmanuelle,

Tu es une fille incroyable avec un tempérament de feu. Je suis sur que tu feras un très bon médecin car ton enthousiasme et ta joie de vivre peuvent redonner courage à n'importe qui.

A Théophane,

Choisir sa voie n'est pas toujours pas une tâche facile mais je suis sur que tu trouveras un domaine ou une spécialité qui te combleras. Garde confiance en toi et tu accompliras tout ce que tu veux.

A Aristée,

Tu es mon petit frangin et je suis désolé de ne pas pouvoir passer assez de temps avec toi. Tu es le bienvenu quand tu le désires sur Grenoble. Tu m'impressionnes vraiment dans tous les projets que tu as entrepris et je pense que de belles opportunités s'offriront à toi.

A Aude,

Ces quelques mois avec toi ont été incroyables. Merci de m'avoir soutenu pendant la fin de ma thèse. Je pense enfin avoir trouvé la fille que j'ai cherchée pendant toutes ces années. Je t'aime …

A mes grands parents maternels,

2 filles, 9 petits enfants, 1 arrière petit enfant : je pense que vous pouvez être fier d'avoir constitué une si belle communauté. Votre réussite, résultat d'un travail acharné, sera toujours un exemple pour moi.

A mes grands parents paternels,

Même si nous ne nous voyons que trop rarement, je pense fort à vous et votre soutien est très important pour moi.

A Pascale, Laurent, Claire, Louis, Anaïs et Jean

Nous avons passé ensemble des moments inoubliables que je ne pourrai jamais oublier. Je vous souhaite à tous beaucoup de bonheur.

A Daniel, Corinne, Amandine et Bérangère

A Sébastien B.,

Depuis le début de cette thèse, tu as toujours été là dans les bons comme dans les mauvais moments. Je sais que je peux compter sur toi. Relâche cependant un peu la pression et la vie n'en sera que plus belle.

A Jérémy et Angélique,

Angélique, je te connais depuis plus de 8 ans; Jérémy, tu es la preuve vivante que de longues années ne sont pas nécessaires à la constitution d'une réelle amitié.. Vous formez tous les deux un couple magnifique et je suis fier de vous avoir comme amis. Vous comptez vraiment pour moi, je vous souhaite tout le bonheur que vous méritez.

A Jonathan,

La distance n'a aucun impact sur notre profonde amitié ; j'espère que tu pourras rapidement te rapprocher d'Adéla.

A Othman,

Je peux tout résumer avec cette seule phrase : "Doc, toi t'es un bon. Non non non, fait pas ton modeste Doc, t'es vraiment un bon. Non Doc, j'insiste, toi t'es vraiment un bon...", Paul Vitti (Robert de Niro). Ne change pas, tu es un véritable ami.

A Sylvain et Céline, Myriam et Fabien,

Je ne compte plus les bons moments passés ensemble ; je vous souhaite à tous énormément de bonheur.

A Carine et Victor,

Je vous remercie pour tous les moments qu'on a passés ensemble, vous êtes un couple formidable et vous comptez très fort pour moi.

A Marion et Thomas,

Merci de m'avoir choisi comme parrain de cœur pour Nina, vous avez une famille magnifique et je vous souhaite tout le bonheur que vous méritez.

A Ricardo,

800km, 8h de route; on peut dire que t'as mis une certaine distance avec Grenoble. Cependant, notre amitié est bien plus forte que ça. En attendant de se voir, je te souhaite énormément de bonheur.

A Romain S.,

Notre amitié remonte à de nombreuses années et ne s'est que renforcée durant tout ce temps. Te revoir de temps en temps est un vrai plaisir. Bon courage pour la suite.

A Benoit D.,

On ne se connait pas depuis très longtemps; ton incroyable bonne humeur est une véritable source de décompression

A Coralie,

Je suis fier de ce que tu as accompli depuis ces dernières années ; je te souhaite énormément de bonheur avec Mathieu.

A mes amis du CEA : Sylvain G., Ahmed, Guillaume B., Sahar, Jérémy C., …

A tous ceux que j'ai rencontré pendant mes études : Stéphanie, Florie, …

***Au groupe des copinous** : Samuel, Ben, Antoine L., Gildas, Mélanie, Aurélien, Pascal, Dounia, Guillaume, Juliette, Thomas, Selma, Stéphane, Pierre, Romain, Nicolas, Mélina, Muriel, Sebastien B., Julien, Fanette, Cédric, Johan, Johanna*

***A mes amis de l'ESISAR** : Alexis, Stéphane, Benoit M., Benoit S. Emilie, Fabien D., Fabien P., Thieux, Fred, …*

***A mes amis brésiliens** que j'ai connu à l'ESISAR ou pendant ma thèse : Euler, Evaneska, Vitor, Gabriel, …*

***A tous mes amis Bassois** : Marion F., Alexandre, Laurent R., Christelle G., Charlotte P., Florian, …*

A mes amis judokas

A mon nouveau laboratoire d'accueil, le LITUS

RESUME

L'avènement des communications en champ proche pour les transactions entre objets portables téléalimentés de type RFID pose un problème de sécurité. En effet, ces communications supportent non seulement la fonction de transfert d'information, mais aussi celle de transfert de puissance d'alimentation et d'horloge vers l'objet nomade. La sécurité des communications repose sur l'authentification des parties, l'intégrité des données et leur confidentialité. En général ces objets téléalimentés sont dits à ressources rares : c'est-à-dire que leur puissance de calcul et leurs possibilités pour se protéger sont limitées

Ces caractéristiques font peser des menaces importantes sur la sécurité du lien sans contact et sur la protection des données personnelles parmi lesquelles quatre sont essentielles :

1) L'espionnage de la communication.

2) L'attaque en relais : L'intégrité de la communication peut être mise en danger par l'utilisation d'un système pouvant relayer à grande distance les commandes d'un lecteur RFID à une carte RFID. Les messages peuvent alors être écoutés, voire modifiés. La détection de la présence de tels dispositifs devient primordiale.

3) L'activation à distance d'une carte RFID.

4) Le déni de service.

L'objectif de cette thèse sera de trouver des contre-mesures impliquant la couche physique et évitant la modification des normes actuelles à la fois dans les dispositifs de type étiquettes électroniques RFID et dans les téléphones portables de type NFC.

Mots-clés : Sans contact, authentification, espionnage de la communication, attaque en relais, étiquettes électroniques, RFID, confidentialité, NFC, intégrité

ABSTRACT

The arrival of the near field communications for transactions between portable remotely powered devices using RFID technology presents a problem. In fact, these communications provide not only an informative function but also a power and clock transfer function to the contactless device. Communication security is based on authentication protocols, security data integrity and confidentiality. Most of these remotely powered devices have low resources and then low defense against attackers. These features create a threat for contactless communications security and privacy data protection. Four types of attack exist:

1) Eavesdropping

2) Relay attack : Communication integrity can be in danger with the use of systems that can relay RFID reader commands to a RFID card. Transactions can be spied or even worse can be modified in case of a man-in-the-middle attack.

3) Skimming : Activation and reading of a contactless card from a distance.

4) The denial of service.

The objective of this thesis is to find countermeasures using the physical layer in RFID contactless devices and in NFC mobile phones while avoiding the modification of actual standards.

Keywords: Contactless, RFID, NFC, integrity, authentication, eavesdropping, relay attack, electronic card

TABLE DES MATIERES

PREAMBULE

Depuis quelques années, il apparaît un nouveau système d'identification que l'on retrouve en particulier dans les zones d'accès sécurisées et dans les transports en commun. Cette technologie, utilisant les ondes radios comme support de communication entre deux dispositifs, est actuellement utilisée par des dizaines de millions de personnes chaque jour à travers le monde.

Le déploiement rapide de cette technologie et la mise en place d'applications nécessitant un fort niveau de sécurité telles que le paiement ou l'accès à des zones sensibles exigent de ces systèmes une sécurisation importante du lien sans contact. D'autre part, les utilisateurs de cette technologie, dont les failles sont amplifiées par les médias, s'inquiètent de plus en plus de l'effet d'une utilisation massive de cette technologie sur leur vie privée. Chaque dispositif sans contact, en plus d'un identifiant unique permettant de tracer un individu, peut contenir aussi des données confidentielles liées à la vie privée des individus telles que les données bancaires ou personnelles. A l'origine, les technologies d'identification et les normes correspondantes n'ont cependant pas ou peu été développées dans l'optique de sécuriser la communication ou de protéger les données sensibles de ses utilisateurs.

Il est aujourd'hui nécessaire de combler les manques liés à l'absence de sécurisation des systèmes sans contact. Dans un premier temps, il sera nécessaire d'identifier les attaques propres au lien sans contact de façon à définir leurs premières caractéristiques et les risques liés à ces attaques. Dans un deuxième temps, certaines attaques seront implémentées de façon à identifier le matériel nécessaire par un attaquant et les limites liées à ces attaques. Enfin, l'objectif principal de l'étude sera de trouver des contre-mesures simples et compatibles avec les normes existantes ; ces contre-mesures feront l'objet de démonstrateurs.

INTRODUCTION : ENJEUX ET OBJECTIFS

Nous présentons dans cette introduction le contexte lié à la mise en place de cette thèse intitulée « sécurisation de la couche physique des communications sans contact de type RFID et NFC ».

1. Une première approche des technologies sans contact

Les technologies sans contact, voir la figure 1, restent difficiles à définir, dans le sens où il existe une grande variété de systèmes dits sans contact. Cette technologie est basée sur l'émission d'un champ électromagnétique contenant des données accessibles par un ou plusieurs systèmes de réception appelés transpondeurs.

Figure 1 – Exemples de systèmes sans-contact

C'est le champ électromagnétique, voir la figure 2, qui sert de support à l'information transmise par le système émetteur ainsi que pour la réponse du transpondeur. Ce même champ électromagnétique peut dans le même temps fournir l'énergie nécessaire au transpondeur pour fonctionner.

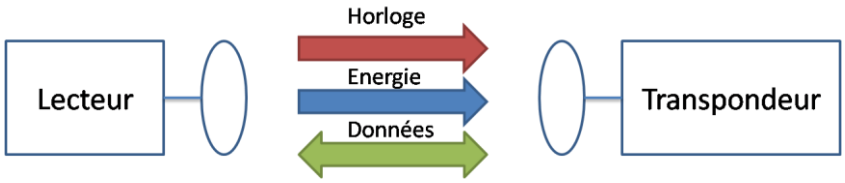


Figure 2 – La transmission d'informations et d'énergie dans un système sans contact

Les technologies sans contact sont nées dans les années 40 à la fin de la seconde guerre mondiale. C'est la combinaison de deux technologies : la radio et le radar. A l'époque, cette technologie est destinée à l'identification des avions alliés. Ce système, appelé IFF (Identify : Friend or Foe), est encore utilisé pour le contrôle du trafic aérien. Cette technologie est restée à usage militaire jusque dans les années 80, où d'importantes avancées technologiques ont permis la réalisation d'un transpondeur sans une source d'énergie embarquée.

Aujourd'hui, les technologies sans contact et RFID sont utilisées à grande échelle et touchent tous les domaines d'applications dont voici quelques exemples (figure 3) :

- Le paiement : Déjà utilisé aux Etats-Unis et au Japon, le paiement par cartes sans contact commence à arriver en Europe.
- Les cartes de transport : Depuis quelques années déjà, les technologies sans contact sont utilisées dans les transports en commun. L'utilisateur utilise sa carte pour s'authentifier, pour valider son titre de transport et recharger cette même carte. En 2008, 3,4 millions de titres de transport étaient utilisés.

- Les documents d'identité : Les nouveaux passeports biométriques possèdent une puce sans contact qui contient des informations telles qu'une photo d'identité, l'empreinte digitale,…
- Les implants : Les animaux (bétail et compagnie) peuvent se faire implanter une puce qui peut contenir des informations sur l'animal en question. Certaines puces développées par Verichip peuvent être implantées dans le corps humain pour le suivi pendant une hospitalisation par exemple.
- La logistique : Depuis plusieurs années, la technologie RFID est en attente de remplacer les codes-barres. Le coût est cependant encore trop élevé pour qu'elle soit utilisée à grande échelle dans les magasins de distribution. Cependant, les avantages de l'utilisation d'une telle technologie sont nombreux : suivi du produit, vue indirecte pour authentifier le produit, …. Cette technologie est déjà utilisée dans le cadre de la logistique de produits manufacturés.

Figure 3 – Exemples d'applications visées par le sans contact

2. Sécurité et vie privée

L'utilisation d'ondes électromagnétiques pour transmettre des données entre deux dispositifs rend cette technologie intrusive et vulnérable aux attaques basées sur l'utilisation de la radiofréquence :

- Il est possible d'écouter une communication entre des systèmes sans contact puisque le support de communication est l'air et que les ondes se propagent dans toutes les directions. On appelle cette attaque « eavesdropping », que l'on peut traduire par espionnage d'une communication.
- Un dispositif passif n'est pas maître de l'énergie qu'il utilise puisque c'est le lecteur qui l'alimente par son champ radiofréquence. Cette vulnérabilité ouvre la voie pour des attaques de déni de service.
- Une carte sans contact est le plus souvent passive et elle ne possède pas d'interrupteur ON/OFF. Un utilisateur ne peut pas activer ou désactiver l'accès à la mémoire d'une carte sans contact dont il est le propriétaire. Un attaquant peut donc activer à distance une carte sans contact de manière transparente et sans l'autorisation de son propriétaire. On appelle cette attaque « skimming », que l'on peut traduire par activation à distance.
- L'horloge utilisée par la carte sans contact est fournie par le lecteur. Un attaquant peut utiliser cette faille pour accélérer ou interrompre les opérations de traitement et les différents protocoles de la carte sans contact.
- Les protocoles d'anticollision sont utilisés par les lecteurs pour connaître l'identifiant d'une carte sans contact lorsque plusieurs transpondeurs sont présents dans son champ radiofréquence. Ce type d'identification peut entraîner des problèmes au niveau de la vie privée des utilisateurs.

Les vulnérabilités introduites par le lien sans contact sont les vecteurs pour de potentielles attaques entraînant des risques importants pour la sécurité du système et la vie privée de ses utilisateurs. La récupération de données par l'utilisation des attaques d'espionnage ou d'activation à distance introduit en particulier quatre risques pour la vie privée de ses utilisateurs.

- Traçabilité : Chaque carte sans contact ou étiquette possède un identifiant absolument unique ; deux paquets de céréales identiques possèdent deux identifiants différents. Il est possible de connaître l'identifiant d'un produit en espionnant une communication ou en activant le transpondeur apposé sur ce produit. De cette manière, il est possible de tracer une personne en récupérant les identifiants des produits détenus par la personne espionnée en plaçant des lecteurs de transpondeurs à différents endroits.
- Spam : Il est possible de se faire apposer un « marqueur » par une personne mal intentionnée ; cette personne peut alors suivre nos déplacements ou obtenir des informations privées sur notre mode de vie, notre personnalité,... Ces données récupérées peuvent être ajoutées dans une base de données de façon à être vendues à des marchands ou autres. Ces informations peuvent ensuite être utilisées pour mieux connaître nos habitudes de consommation et nous proposer des objets en fonction de nos préférences.
- Terrorisme, profilage : Les informations récupérées sur un « marqueur » ou sur un transpondeur par espionnage ou activation peuvent être utilisées pour classer ou agresser des personnes selon des critères politiques, ethniques, ...
- Puce sous-cutanée : A l'heure de la miniaturisation des systèmes électroniques, l'injection de puces RFID dans le corps est déjà une réalité. A l'état microscopique, il serait possible de tracer toute une population de façon totalement illicite ce qui met en danger la vie privée des individus.

Voici deux affaires qui ont créées la polémique aux Etats-Unis :

Gillette : En 2003, face à la recrudescence des vols de lames de rasoir dans les magasins, Gillette met en place un système à base de puce RFID. Celui-ci permet de prendre en photo l'acheteur à la prise du produit dans les rayons et à sa sortie du magasin. Les deux photos sont alors comparées et l'ordinateur vérifie que le produit a été payé.

Cette affaire a fait scandale aux Etats-Unis car le système permet de tracer un individu et de le prendre en photo sans son consentement.

Benetton : Toujours en 2003, l'entreprise Benetton incorpore des puces RFID dans les habits de sa marque de façon à tracer ses vêtements de l'usine au point de vente. L'objectif n'est pas de surveiller les acheteurs, mais de faciliter les inventaires et d'améliorer la gestion des stocks. Cependant, ces puces sont invisibles et ne sont pas désactivées lors de l'achat du produit, ce qui inquiètent les associations qui luttent pour la protection de la vie privée.

La législation française prévoit déjà un certain niveau de protection de la vie privée ; elle interdit par exemple l'identification à l'insu de l'individu. Chaque appareil utilisant la technologie sans contact doit être visible par l'individu et doit indiquer qu'il permet de lire les transpondeurs. Cependant, aux yeux de certaines associations, cette loi ne protège pas assez l'individu et ses informations personnelles.

De nombreuses associations proposent même le boycott de cette technologie, car elles l'estiment contraire à la liberté des individus.

L'association américaine **CASPIAN** (consommateurs contre la violation de la vie privée par les supermarchés) a par exemple dénoncé les principes de cette technologie et a déjà incité au boycott de plusieurs marques de la grande distribution.

3. Contexte économique

En 2009, malgré la crise économique, la croissance des technologies sans contact continue de croître, voir la figure 4, avec une valeur du marché mondial qui a atteint les 5.56 milliards de dollars selon IDTechEx [IDTECH]. Ce chiffre montre une croissance à deux chiffres, proche de 10 % puisque le chiffre d'affaires était de 5,25 milliards de dollars en 2008. Les technologies sans

contact restent sûres et devraient continuer de croître dans les années futures, ce secteur devrait atteindre une croissance de près de 30 % autour de 2013 [FilRFID].

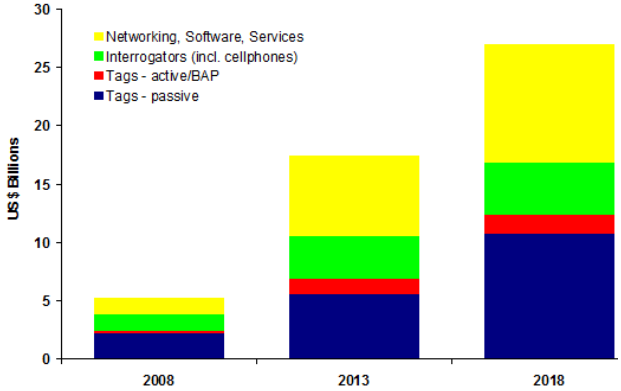


Figure 4 – Croissance du marché du sans contact [IDTECH]

L'Europe reste cependant un peu en retrait dans l'utilisation de ces technologies, voir la figure 5. La France est particulièrement en retard ; seules 2% des entreprises françaises utilisent cette technologie. Cette problématique, liée à la sécurité et à la vie privée des individus, a un impact fort sur le ralentissement de cette croissance alors que le Japon et les Etats-Unis utilisent déjà ces technologies comme moyens de paiement.

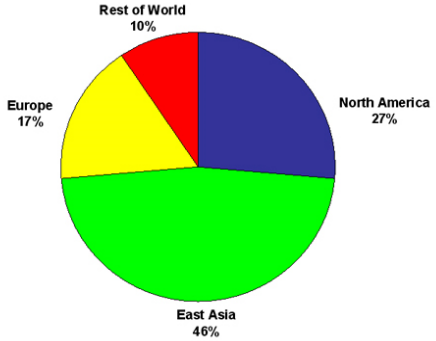


Figure 5 – Marché mondial par continent en 2008 [IDTECH]

Les autres facteurs de ce ralentissement sont le prix encore élevé d'une étiquette RFID par rapport à un simple code-barre, un investissement trop lourd et de trop gros changements dans la chaîne logistique. Les industriels regardent donc l'arrivée de cette technologie avec un peu de recul et chacun évite de faire le premier pas. Certaines entreprises ont d'ailleurs été la cible des associations anti-RFID (Benetton, Gillette, Métro,…) à la suite de l'utilisation de RFID dans leurs produits. Toutes ces craintes face aux technologies d'identification ont un impact économique très fort à tous les niveaux puisque la RFID représente quand même de très bonnes opportunités autant pour le consommateur que pour l'industriel.

4. Objectifs de la thèse

Dans une thématique sécurité, cette thèse s'inscrit dans la prévention des risques potentiels liés à l'utilisation des technologies sans contact. Ces dernières présentent de nombreuses failles technologiques, de par l'utilisation d'ondes radiofréquences et du manque de contraintes des normes actuelles définissant ce type de communications.

Les enjeux de cette thèse sont conséquents ; le manque de confiance des utilisateurs dans cette technologie et les problèmes liés à la sécurité et à la vie privée des individus ont pour conséquence une croissance faible des technologies sans contact L'objectif principal de cette thèse est donc de trouver des solutions garantissant à l'utilisateur que cette technologie est sûre et qu'elle ne présente aucun danger au niveau de la sécurité des personnes et de leur vie privée.

Cette thèse peut être divisée en plusieurs parties : bibliographie, conception, identification, mise en œuvre.

La première phase est la bibliographie : elle consiste à comprendre les phénomènes et les caractéristiques du lien sans contact, les failles de cette technologie et identifier les attaques existantes. De la même façon, les solutions proposées actuellement dans la littérature doivent être analysées pour comprendre leurs faiblesses.

La phase de conception a pour objectif la mise en place de deux des principales attaques au niveau de la couche physique des systèmes sans contact, soit l'eavesdropping (écoute à distance) et l'attaque relais. L'objectif est de trouver les limites de chacune de ces attaques en termes de distance ou de délais, pour pouvoir ensuite tester nos contre-mesures sur ces systèmes.

En effet, l'objectif majeur de la thèse est d'identifier des contre-mesures impliquant la couche physique et évitant la modification des normes actuelles à la fois dans les dispositifs de type sans contact et NFC. Ces contre-mesures doivent exiger une faible puissance de calcul au niveau de la carte. En effet, ces systèmes sans contact sont dits à ressource rare ; seul le lecteur peut traiter des données. Lors de cette recherche de solutions, nous nous concentrerons sur l'attaque relais, car cette attaque a la particularité de ne pouvoir être détectée ou rendue inutile par des protocoles cryptographiques, contrairement aux attaques skimming et eavesdropping.

Les contre-mesures devront ensuite être mises à l'état de prototype de façon à évaluer au mieux la sécurité apportée par de tels systèmes, c'est la phase de « mise en œuvre ». Pour implémenter les contre-mesures sur des systèmes sans contact, un lecteur et une carte « ouverts », développés au sein du CEA, seront utilisés.

Chapitre I. Etat de l'art

PARTIE I. LES TECHNOLOGIES SANS CONTACT, RFID ET NFC

Une rapide présentation des technologies sans contact, RFID et NFC a été réalisée dans l'introduction ; nous allons ici détailler plus précisément chacune de ces technologies

1. Introduction

Le tableau I-1 regroupe l'ensemble des solutions sans contact et RFID et leurs fréquences de fonctionnement. Les caractéristiques de ces différents systèmes telles que la vitesse de transmission des signaux ou la distance de lecture sont rappelées.

Tableau I-1 – Caractéristiques des différents systèmes en fonction de leur fréquence de fonctionnement

	Fréquences utilisées	Type de couplage	Distance de lecture	Vitesse de transmission	Normes correspondantes	Applications
Low Frequency (LF)	125 – 135 kHz	Couplage inductif	Jusqu'à 1.2m	lente	11784, 11785 et 14223	Capteurs, systèmes anti-démarrage, systèmes d'alarme, suivi d'objets, …
High Frequency (HF)	13.56 MHz	Couplage inductif	ISO14443 : jusqu'à 30 cm ISO15693 & ISO18000 : jusqu'à 3 mètres	dépend de la norme	14443, 15693 et 18000	Porte-monnaie électronique, transport, contrôle d'accès, traçabilité, …
Ultra High Frequency (UHF)	865 - 956 MHz	Couplage électrique	Jusqu'à 10m	rapide	18000	Identification, système de télécommande
Microwave	2.45 et 5.8 GHz	Couplage électrique	Plus de 15m	très rapide	18000	Télépéage autoroutier, …

Dans la suite de cet état de l'art, nous nous intéresserons principalement aux systèmes hautes fréquences fonctionnant à 13.56 MHz [FIN2003, PAR2001, PAR2003]. On distingue trois grandes familles d'applications pour ces dispositifs à couplage inductif :

- Les technologies RFID : identification d'objets
- Les technologies sans contact : identification de personnes
- Les technologies NFC : transferts de données

La suite du document introduit chacune de ces applications et leurs systèmes de fonctionnement

2. Les différentes technologies RFID, sans contact et NFC

A. La technologie RFID

La technologie RFID (Radio Frequency IDentification) est une méthode d'identification d'objets à distance utilisant les ondes radiofréquences.

Les transpondeurs utilisés en RFID sont aussi appelés tags. Ils sont le plus souvent constitués d'une antenne et d'un circuit intégré permettant le traitement et le stockage d'informations, la modulation et la démodulation du signal. En RFID, les tags sont le plus souvent passifs et donc complètement téléalimentés par le lecteur.

Une étiquette RFID, voir la figure I-1, contient au moins un identifiant unique, mais le plus souvent contient d'autres informations sur l'objet tagué.

Figure I-1 – Exemples de tags RFID

L'ISO 18000, comprenant le standard EPC, utilise la technologie RFID. EPC signifie Electronic Product Code (code produit électronique) ; c'est un code unique permettant d'identifier un objet [ISO18000-3].

Les applications liées à ce standard sont multiples, mais la principale reste l'identification et la traçabilité d'objets pendant tout ou une partie de leur durée de vie. Il est ainsi possible de mémoriser de nombreuses informations dans une puce RFID puis par lecture connaître les caractéristiques du produit : provenance, date de création, ... Son objectif principal est donc de remplacer le code-barre et de disposer d'un identifiant unique et universel pour chaque objet présent dans la chaine logistique de chaque entreprise du monde.

Le principal frein à l'utilisation massive de la RFID est un prix supérieur à celui d'un simple code-barre.

B. La technologie sans-contact

Une smartcard est une carte à puce de type carte bancaire qui embarque un circuit intégré permettant de traiter des informations et de les mémoriser. Une carte sans contact est différente de la smartcard au niveau de sa couche physique car les signaux échangés entre la carte et le lecteur sont transmis par ondes radiofréquences.

Une carte sans contact a des dimensions type ID1 (carte à puce) définies par la norme ISO 7810. Elle possède aussi une unité de cryptographie qui assure plus de sécurité que pour un simple tag.

Les cartes sans contact, voir la figure I-2, sont majoritairement utilisées pour l'identification et l'authentification de personnes (passeport, carte de transport, ...).

Figure I-2 – Cartes sans contact et applications

Les normes définissent actuellement des débits allant de 106 à 848 Kbits/s. Il existe plusieurs distances de fonctionnement définies par des normes :

- ISO 14443 [ISO14443-1], [ISO14443-2, ISO14443-3, ISO14443-4] (Proximity cards) : Elle définit deux types de communications et permet une distance d'activation jusqu'à 10 cm.

- ISO 15693 [ISO15693-1, ISO15693-2, ISO15693-3] (Vicinity cards : Elle permet une distance d'activation jusqu'à 1 m.
- ISO 10536 [ISO10536-1, ISO10536-2, ISO10536-3] (Close-coupled cards) : Elle permet une distance d'activation de 2 cm.
- La norme 10373 [ISO10373-6] permet de définir les moyens de tests des normes énoncées ci-dessus.

C. La technologie NFC

La technologie NFC (Near Field Communication) est une technologie sans contact au même titre que la technologie RFID. L'objectif initial était de combiner la fonction lecteur et la fonction transpondeur dans un même dispositif. La fonction principale de la technologie NFC est d'interagir avec un environnement donné (cartes d'accès, paiements sécurisés, téléchargement de données), voir la figure I-3.

Figure I-3 – NFC et applications

Il existe trois modes de communication en NFC :

- Le mode lecteur : C'est une communication entre un dispositif NFC qui agit comme un lecteur et un transpondeur standard. Ce mode permet au lecteur d'échanger des informations avec le transpondeur. Par exemple, ce mode de communication peut permettre de lire un transpondeur sur une affiche de cinéma afin d'obtenir les horaires des séances ou l'adresse du cinéma qui le diffuse (un débit plus important pourrait permettre de télécharger la bande-annonce).
- Le mode « émulation de carte » : C'est une communication entre un lecteur standard et un dispositif NFC vu par le lecteur comme un simple transpondeur. Ce mode peut être utilisé sur un téléphone portable pour intégrer des fonctions de paiement ou d'accès sécurisés.
- Le mode P2P : Il permet l'échange de données entre deux dispositifs NFC. Il peut être utilisé pour échanger des données entre plusieurs machines intelligentes dotées de la technologie NFC, initialiser une communication Bluetooth, ...

Deux normes définissent le protocole NFC, voir la figure I-4 :

- La norme NFC-IP1 (ECMA 340 [ECMA340] et ISO 18092 [ISO18092]) définit le mode P2P : Cette norme doit être compatible avec la norme ISO 14443-A et Felica (norme Sony appelée aussi type C). A l'heure actuelle, on observe quelques incompatibilités entre la norme NFC-IP1 et la norme ISO 14443-A. De nombreuses discussions aux comités de normalisation ont lieu pour étudier la convergence de ces deux normes.
- La norme NFC-IP2 (ECMA 352 [ECMA352]) définit le mode lecteur : la norme impose que les dispositifs NFC soient compatibles en tant que lecteurs de transpondeurs définit par les normes ISO14443 type A et B et ISO 15693.

Aucune norme actuelle ne définit le mode émulation de transpondeur. Cependant, le NFC Forum, un comité composé de grands acteurs de la RFID, a déjà développé des solutions et leurs spécifications.

Les procédures de tests au niveau protocole et interface sont définies respectivement par les normes ECMA 362 [ECMA362] et ECMA 356 [ECMA356]. La norme NFC-WI (ECMA 373) [ECMA373] permet de définir l'interface entre le front-end RF et la partie sécurisée.

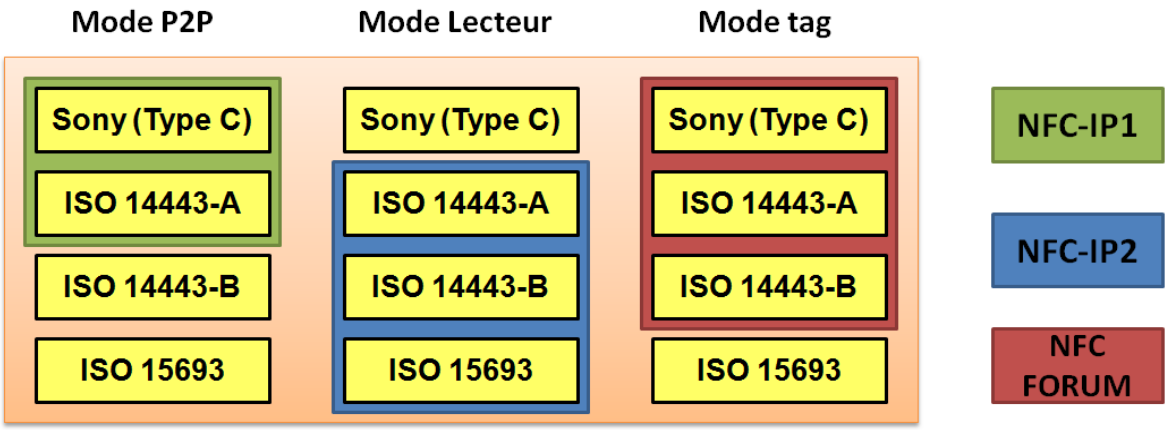


Figure I-4 – Normes et NFC

3. Les principes d'un système sans contact

A. Le système sans contact

a. Lecteur et transpondeur

Le système sans contact est généralement composé d'un lecteur et d'une ou plusieurs cartes sans contact (figure I-5)

Le lecteur (station de base) est l'élément maître de la communication ; il gère les échanges avec le transpondeur en lui envoyant des requêtes. De plus, il peut fournir l'énergie nécessaire au transpondeur pour s'alimenter.

Le système lecteur peut être décomposé en une partie analogique et une partie numérique gérée par un microcontrôleur. La partie la plus complexe est la partie analogique et/ou numérique qui comprend le front-end RF et l'interface avec le microcontrôleur. Cette partie inclut le codage et la modulation des données, ainsi que la génération d'une porteuse permettant d'alimenter la carte. La réception du signal est très difficile à implémenter, car le lecteur doit réceptionner un signal de faible amplitude généré par la modulation de charge de la carte dans un signal de très forte amplitude (la porteuse du signal). La chaine de réception comprend généralement une importante partie traitement du signal (filtrage, amplification, démodulation et décodage du signal) ainsi que de mise en forme des signaux décodés. Le microcontrôleur assure la gestion du protocole de communication (émission, réception, gestion de collisions, …) et les différentes interfaces possibles (hôte, écran, …).

Le transpondeur est composé d'une puce et d'une antenne résonante. Il se contente de répondre aux requêtes du lecteur et de permettre un accès en écriture et en lecture à sa mémoire. Le lecteur récupère des données contenues dans la mémoire du transpondeur. Le transpondeur répond de manière synchrone avec l'horloge de la porteuse du lecteur. Le transpondeur dispose aussi d'un système de gestion d'énergie permettant la récupération d'une alimentation à partir du champ RF généré par le lecteur. Le tag possède très peu de ressources de calcul et ne peut pas effectuer de grosses opérations.

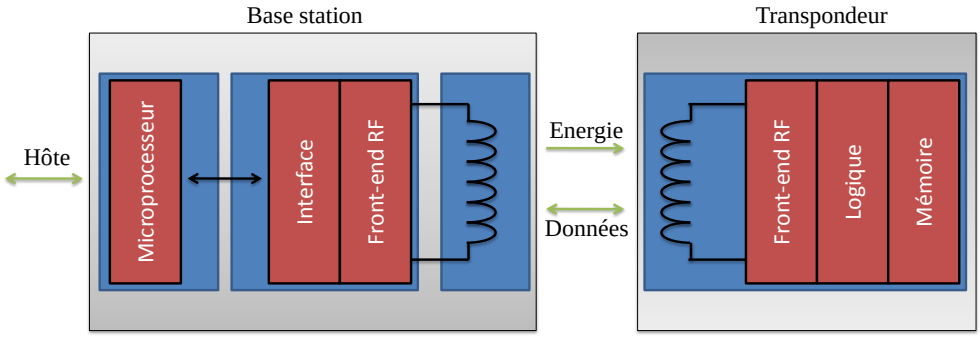


Figure I-5 – Structure d'un système sans contact [PAR2003]

b. Dispositif actif et passif

Un dispositif est dit passif s'il ne dispose d'aucune source d'alimentation en interne. Il est téléalimenté par l'énergie provenant du lecteur.

Un dispositif est dit actif s'il comporte une source d'énergie en interne. Il est donc plus autonome et capable d'avoir des fonctions plus consommatrices en énergie.

B. Communication et transfert d'énergie

Dans la plupart des systèmes utilisant le couplage inductif, le lecteur doit fournir toute l'énergie nécessaire au fonctionnement de la carte. L'exemple le plus simple de transmission d'énergie par couplage inductif est le transformateur. Les deux bobines sont électriquement isolées l'une de l'autre. Ce type de système permet pourtant de transmettre de l'énergie par couplage entre les deux bobines. Un courant est induit dans le secondaire lorsqu'un courant est injecté dans la boucle primaire. Ce courant est fonction du courant dans la bobine au primaire et d'autres paramètres liés au couplage. Dans le cas des systèmes sans contact, la résonance au primaire et au secondaire permet d'augmenter de façon significative le rendement puisque l'énergie transmise va se concentrer sur la carte qui a la même fréquence de résonance que l'émetteur. En pratique, le lecteur crée un champ magnétique en générant une tension sinusoïdale dans son antenne ; ce champ permet d'alimenter la carte, voir la figure I-6.

La transmission de données est réalisée en modulant la tension sinusoïdale (porteuse).

Dans la plupart des cas, cette modulation d'amplitude est réalisée côté lecteur pour la voie montante et côté carte pour la voie descendante. Au niveau de la carte, cette modulation est créée par variation d'une charge résistive ou capacitive.

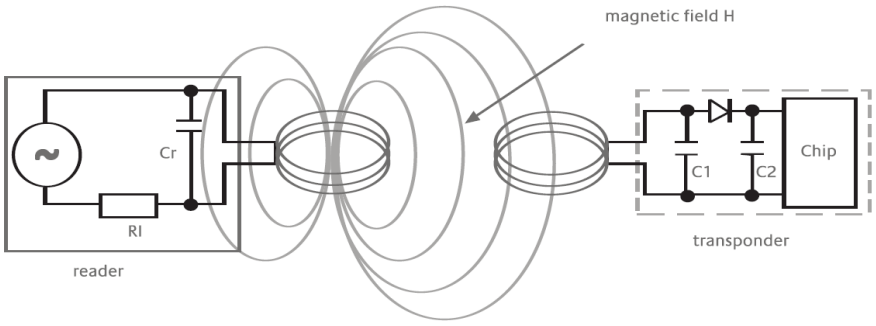


Figure I-6 – Le couplage inductif vu par Klaus Finkenzeller [FIN2003]

PARTIE II. ATTAQUES

Cette partie du document traite des différentes attaques étudiées dans la littérature. Toutes ces attaques sont introduites spécifiquement par le lien sans contact.

1. Eavesdropping (Ecoute à distance)

L'attaque eavesdropping, voir la figure I-7, consiste à écouter une transaction privée entre un lecteur et une carte sans l'accord des protagonistes dans l'intention d'y déceler des secrets. Cette attaque est dite passive, car on n'agit pas sur le système RFID. Cette attaque au niveau de la couche physique est l'une des plus simples à réaliser, car elle ne requiert que très peu de matériel. Une simple sonde de champ et un oscilloscope peuvent suffire à récupérer des signaux à plusieurs mètres de distance. Les trames enregistrées lors d'une attaque eavesdropping vont servir à récupérer des informations plus ou moins importantes. Elles peuvent aussi servir dans le cadre d'une attaque replay (voir Substitution, clonage, replay). Il est bien entendu possible de réaliser des systèmes d'eavesdropping plus complexes avec traitement du signal à l'aide de logiciels tels que Matlab. De nombreuses publications traitent de cette attaque, mais très peu donnent la méthodologie de test utilisée pour obtenir leurs résultats.

Figure I-7 – Attaque eavesdropping

Les premiers résultats d'eavesdropping ont été publiés en 2004 par le NIST (National Institute of Standard and Technology) [HOS2004]. Les chercheurs du NIST ont réussi à récupérer les données confidentielles sur un passeport situé à 9 mètres de leur sonde espionne. Le matériel utilisé par cette équipe était un lecteur du commerce équipé d'une antenne spécifique. Cependant, l'article ne donne que très peu d'informations sur la méthodologie de test et sur les résultats obtenus. Au vu de la distance d'écoute trouvée par le NIST, il semble que seules les données transmises depuis le lecteur vers la carte aient été enregistrées. Leurs résultats montrent aussi que l'ISO14443 type B est plus sensible aux attaques que l'ISO14443 type A.

Dans [FIN2004], des chercheurs du BSI (Office fédéral de la sécurité des technologies de l'information Allemand) montrent qu'il est possible d'écouter une communication RFID entre un lecteur NXP (norme ISO14443 type A) en se plaçant à 2 mètres du lecteur. L'antenne du lecteur et l'antenne du système d'écoute sont placées en deuxième position de Gauss (voir « Position de Gauss » et la figure I-8).

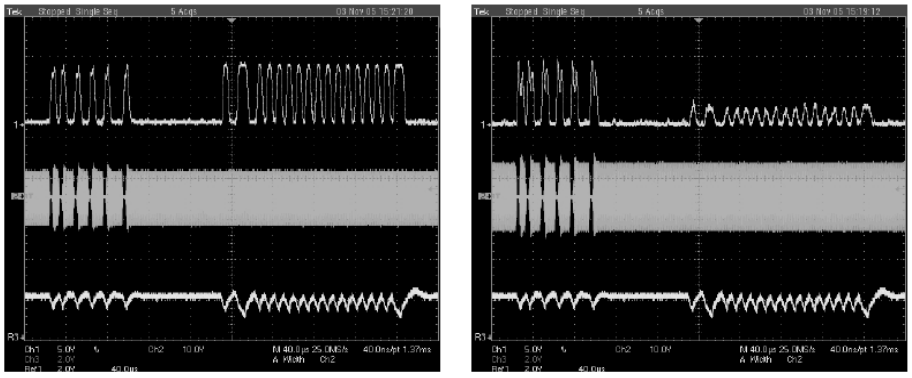
Figure I-8 – Expérimentation de Finke et Kelter [FIN2004]

Le FOIS (Federal Office for Information Security) présente un rapport en 2004 sur les risques liés aux communications sans contact [FOI2004]. Ce rapport ne présente aucune expérience mais regroupe des informations sur les nombreuses mesures d'eavesdropping réalisées. Plus la distance nominale de fonctionnement du système est grande et plus le risque d'eavesdropping est important. Certains protocoles d'anticollision sont un avantage pour l'attaquant utilisant l'eavesdropping car ces protocoles répètent souvent l'identifiant de la carte. Des estimations théoriques basées sur la transmission de puissance entre le lecteur et la carte ont permis de démontrer que :

- La distance d'écoute de la voie montante peut atteindre quelques dizaines de mètres.
- La distance d'écoute de la voie descendante ne peut pas dépasser cinq fois la distance nominale de fonctionnement du système.

En 2006, des chercheurs du NIST réalisent des expériences sur les deux positions de Gauss (voir « Position de Gauss ») [GUE2006]. Ils sont parvenus à espionner une communication sans contact à une distance de 15 mètres pour la voie montante en 2ème position de Gauss et à 6.5 mètres en 1ère position de Gauss. Ces mesures permettent de montrer l'importance de la position des antennes en fonction de la distance d'espionnage. Tous les tests sont réalisés avec un lecteur NXP Pegoda conforme à la norme ISO14443 type A.

Dans [HAN2006], L'auteur présente différents résultats d'attaques sur la couche physique, dont l'attaque eavesdropping. Cette publication reste la plus précise au niveau de la méthodologie de test. Les distances trouvées sont de 4 mètres pour la voie montante et la voie descendante. Le document manque malheureusement de résultats et les mesures ne sont pas assez exploitées, voir la figure I-9.



(a) A5 antenna with 1 W amplifier, $d_p = 15$ cm and $d_e = 75$ cm. (b) A5 antenna with 1 W amplifier, $d_p = 15$ cm and $d_e = 145$ cm.

Figure I-9 – résultats publiés par Hancke [HAN2008-A]

En 2008, G. Hancke publie un nouveau document sur l'attaque eavesdropping [HAN2008-A] et rend public son mémoire de thèse [HAN2008-C]. Ce document complète le premier article en

ajoutant plus de résultats et une meilleure exploitation des données enregistrées. G. Hancke étudie l'attaque pour les différentes normes fonctionnant à 13.56 MHz avec une méthodologie de test très étudiée, voir la figure I-10. L'antenne d'écoute est placée en première position de Gauss à différentes distances de l'antenne d'émission. Le signal est ensuite acquis sur un ordinateur pour être traité.

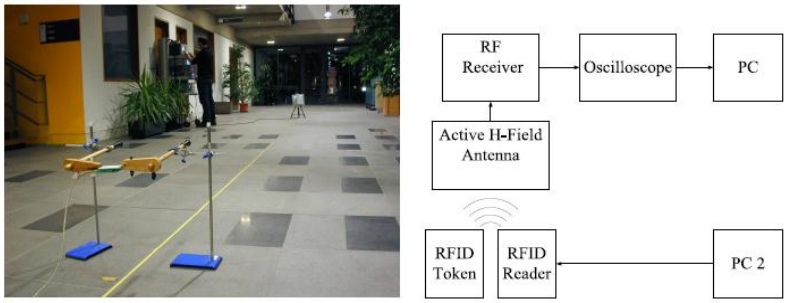


Figure I-10 – Méthode expérimentale

Le tableau I-2 montre les résultats obtenus par Hancke pour les différentes normes à 13.56 MHz pour la voie montante et la voie descendante.

Tableau I-2 – Résultats obtenus par Hancke

	ISO14443-A et ISO15693	ISO14443-B
Lecteur vers carte	> 10 m	3 m
Carte vers lecteur	1 m	3 m

2. Skimming (Activation à distance)

L'attaque skimming, voir la figure I-11, consiste à venir activer et lire une carte sans le consentement de son propriétaire. Cette attaque est dite active, car l'attaquant doit fournir l'énergie nécessaire au fonctionnement de la carte. En général, cette attaque permet de communiquer avec la carte en dehors de sa plage de fonctionnement. La distance de fonctionnement nominal d'un système conforme à la norme ISO14443 est d'une dizaine de centimètres ; l'attaquant doit donc être capable de communiquer avec la carte à une distance supérieure. Les deux principales difficultés liées à cette attaque sont la téléalimentation de la carte et la récupération des données envoyées par la carte. La distance d'activation de la carte est donc énormément limitée par ces paramètres.

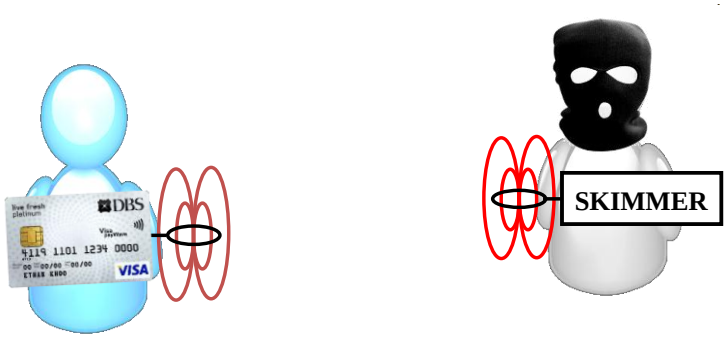


Figure I-11 – Attaque skimming

Le principal objectif de cette attaque est la récupération des données contenues sur la carte, mais ses applications sont multiples (attaque replay, clonage, déni de service,…).

Cette attaque reste difficile à réaliser ; l'attaquant doit être capable d'alimenter la carte tout en modulant son champ pour envoyer les commandes. Un compromis est important entre distance d'activation et récupération des données :

- une antenne avec un coefficient de qualité élevé permettant de générer un champ de forte amplitude avec un minimum de puissance dissipée : besoin d'un important coefficient de qualité d'antenne
- une bande passante assez large pour envoyer les commandes : besoin d'un faible coefficient de qualité d'antenne

Il est possible de réaliser ce compromis en utilisant deux dispositifs équipés d'antennes différentes. La réception des données de la carte est aussi difficile, car le skimmer doit avoir une bonne dynamique pour récupérer la modulation de charge.

Dans [HAN2006], G. Hancke présente les premiers résultats expérimentaux sur l'attaque skimming dans une publication regroupant les trois plus importantes attaques au niveau de la couche physique. G. Hancke réalise des tests de skimming avec plusieurs tailles d'antennes (A3, A4, A5) et plusieurs types d'amplificateurs (0.5W, 1W, 2W, 4W). La distance de lecture maximum obtenue par Hancke est de 27 cm, voir le tableau I-3.

Tableau I-3 – Résultats obtenus pour l'activation de la carte

	0.5 W	1 W	2 W	4 W
A5 (148x210 mm)	15 cm	16 cm	17 cm	19 cm
A4 (210x297 mm)	20 cm	23 cm	23 cm	25 cm
A3 (297x420 mm)	22 cm	25 cm	26 cm	27 cm

Selon G. Hancke, une distance d'activation de 15 cm suffit amplement pour activer la carte d'un individu dans un milieu bondé. Il précise cependant que plus on amplifie la porteuse et plus on a du mal à récupérer le signal sur la voie descendante.

En 2006, I. Kirschenbaum et A. Wool réalisent un système de skimming longue portée pour un coût inférieur à 100 $ à partir de matériel électronique amateur [KIR2006]. Leur document explique chaque détail de la conception de ce dispositif de skimming. Il présente ensuite les résultats obtenus avec leur système, voir la figure I-12.

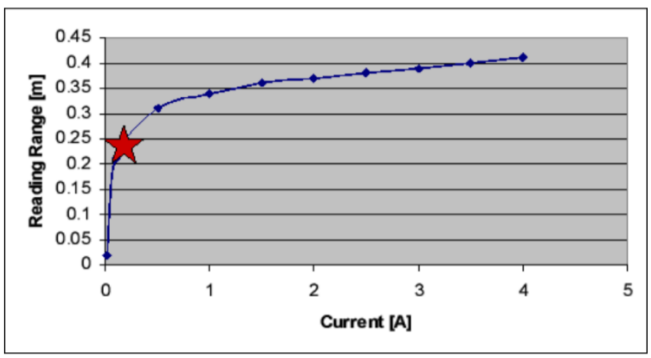


Figure I-12 – Distance de lecture en fonction du courant pour une antenne 40*40cm

Les deux auteurs parviennent à atteindre une distance de 25 cm (plusieurs fois la distance nominale de fonctionnement) en injectant un courant inférieur à 1A dans l'antenne.

3. Attaque relais

L'objectif de l'attaque relais consiste à établir une communication entre un lecteur et une carte sans contact sans le consentement de son propriétaire. La distance entre la carte sans contact et le lecteur est souvent supérieure à la distance nominale de fonctionnement ; le lecteur est pourtant convaincu que la carte sans contact est dans son champ RF.

Le dispositif permettant de réaliser cette attaque, voir la figure I-13, est constitué de deux éléments : un môle et un proxy. Ceux-ci peuvent être reliés entre eux par un lien filaire ou sans fil. Ensemble, ces deux éléments vont relayer les informations entre le lecteur et la carte.

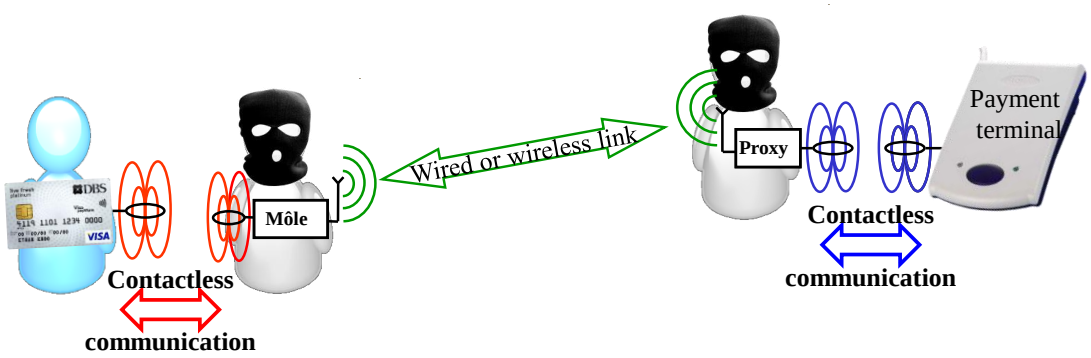


Figure I-13 – Synoptique d'une attaque relais filaire ou sans fil

Le dispositif « môle » doit être placé assez près de la carte de la victime. Il peut être assimilé à un système de skimming ; il a trois fonctions principales :

- Se substituer au véritable lecteur et envoyer les signaux transmis par le proxy à la carte
- Téléalimenter la carte sans contact
- Transmettre les réponses de la carte au proxy

Le dispositif « proxy » est placé à proximité du lecteur, il doit se comporter comme une carte sans contact valide, il a deux fonctions :

- Transmettre les requêtes du lecteur au môle
- Récupérer les données envoyées par le môle et les transmettre au lecteur de manière transparente

Le principal facteur permettant d'obtenir une attaque relais performante est l'amélioration de la distance entre les différents éléments constituant le relais [KFI2005]. Théoriquement, Le proxy peut être placé à 50 m du lecteur et la carte à 50 cm du môle. Ces valeurs ont été calculées théoriquement à partir d'un modèle de système sans contact. La distance entre le môle et le proxy n'est pas limitée puisqu'elle ne dépend que de la technologie utilisée pour faire le lien entre ces deux éléments.

La première réalisation pratique de l'attaque relais sur un système sans contact, voir la figure I-14, montre qu'il est possible de relayer des informations entre un lecteur et une carte séparés de 50 m [HAN2005-A, HAN2008-C].

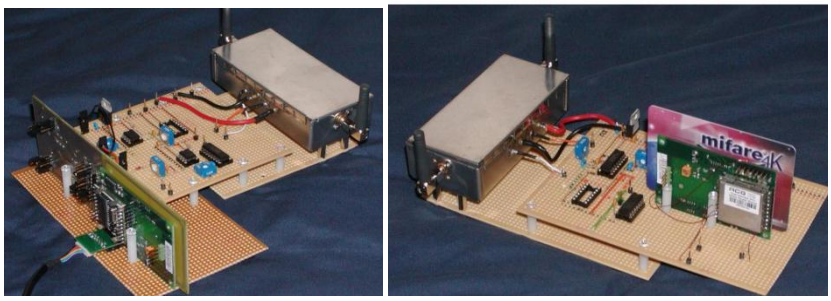


Figure I-14 – Attaque relais selon Hancke

Cependant, on peut noter quelques faiblesses liées à l'architecture de ce système :

- La carte est placée sur le môle lors des expériences, ce qui ne sera pas le cas lors d'une attaque réelle. Aucune information n'est donnée sur la distance d'activation.
- Le retard engendré par le relais est supérieur à 15 us. Cette valeur est importante et pourrait être mesurée facilement par un système sans contact.

L'attaque a été réalisée avec le même succès et un retard équivalent en 2006 [CAR2006].

Depuis cette première attaque réalisée par Hancke, d'autres attaques relais ont été menées en utilisant des protocoles de communication comme la NFC et l'utilisation des réseaux téléphoniques pour transmettre les données entre le proxy et le môle (deux téléphones portables).

Une étude importante a été menée en 2010 par une équipe de chercheurs [FRA2011]. Deux nouveaux types de relais (un relais filaire et un relais sans fil analogique) en mode de communication simplex (transmission dans un seul sens) ont été développés dans le domaine des réseaux véhiculaires. Ils ont alors montré qu'il était possible de relayer les informations entre la voiture et sa clé sur une distance de plusieurs dizaines de mètres. La principale limitation est la distance entre le relais et la clé qui doit être inférieure à 8 mètres. Cette étude est assez proche d'une étude que nous avons menée sur les systèmes sans contact.

Exemple de scénario :

Au Japon et aux Etats-Unis, la technologie sans contact est déjà utilisée pour le paiement. Dans cette thématique, l'attaquant peut, en utilisant l'attaque relais, faire payer ses achats par une victime se trouvant dans la zone d'action du relais. Pour réaliser cette attaque, l'attaquant se dirige vers la borne de paiement tandis que son complice se dirige vers une victime. Lors du paiement, l'attaquant place le proxy sur le terminal de paiement ; son complice rapproche le môle de la victime afin de créer le relais entre la borne de paiement et la carte de la victime. Le vrai lecteur communique donc avec la carte sans se douter qu'elle est placée loin de lui et débite le compte de la victime.

Le même scénario peut être appliqué à de nombreuses autres situations : accès à une zone sécurisée, passage d'une frontière, …

Cette attaque est la plus dangereuse au niveau de la couche physique pour les raisons suivantes :

- La victime n'a pas conscience de l'activation de sa carte puisque cette carte va échanger des données sitôt qu'elle sera téléalimentée.
- L'attaque relais est une attaque au niveau de la couche physique. Les bits codés sont transmis par le relais sans connaître la signification de la trame complète. La norme ISO9798 prévoit un protocole d'authentification pour vérifier que les deux acteurs de la communication connaissent une même clé secrète. Pour des attaques telles que l'eavesdropping ou le skimming, l'utilisation de tels protocoles d'authentification ou de cryptographie permet de limiter les risques. Cependant, il n'est pas nécessaire de connaître la clé secrète pour réaliser une attaque relais. En effet, lors d'une attaque relais, le relais ne modifie et ne décode pas les informations contenues dans les trames. Le relais transmet uniquement les données. Les données cryptées seront transmises de la même façon que des données en clair.
- Les normes sans contact, RFID et NFC imposent certaines contraintes temporelles pour synchroniser les données envoyées par plusieurs tags, en particulier pendant la phase d'anticollision. En pratique, le lecteur ne vérifie pas que la carte répond dans les temps. Un lecteur ou un môle peut spécifier le temps de réponse de la carte et l'augmenter jusqu'à 5 s [HAN2009, KFI2005] ; ce délai permet l'utilisation de relais beaucoup plus complexes.

Dans [HAL2007], L'auteur montre que l'authentification d'une clé secrète par le lecteur n'est pas une preuve de la validité d'une carte sans contact. L'article montre les faiblesses de la norme ISO14443 qui autorise des temps de réponse pour la carte trop élevés et permet à un attaquant de placer un relais entre la carte et le lecteur lorsqu'il le désire.

4. Attaque man-in-the-middle

L'attaque Man-in-the-Middle, voir la figure I-15, est une version plus évoluée de l'attaque relais. En effet, cette attaque possède des caractéristiques similaires à l'attaque relais : l'objectif consiste à transmettre les données entre le lecteur et la carte en passant par le relais. La principale différence de cette attaque est que les bits échangés entre le lecteur et la carte vont être modifiés durant le passage dans le relais.

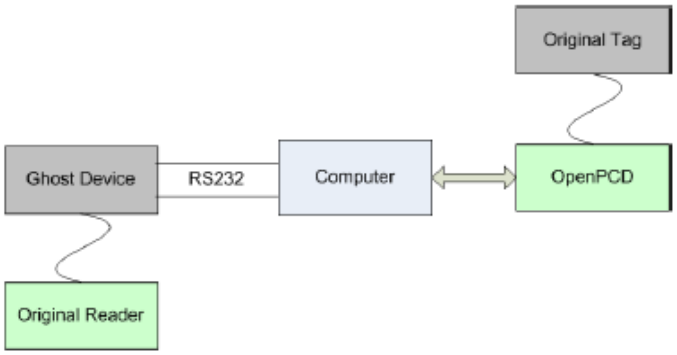


Figure I-15 – Attaque Man in the middle vu par Roel Verdult [VER2008]

Les données peuvent être modifiées directement sans démoduler le signal, mais cette technique ne permet pas de modifier les bits de n'importe quel codage ; l'intérêt est limité puisque l'on ne décode pas le signal et que l'on ne sait pas ce qui est transmis. Une autre solution consiste à décoder le signal, l'interpréter et modifier les bits en conséquence. Le principal avantage de l'attaque relais est sa transparence vis-à-vis de la cryptographie ; l'attaque man-in-the-middle ne possède pas cet avantage. L'attaquant a besoin de connaître la signification de la trame s'il veut pouvoir modifier les données qu'elle contient. Dans ce cas, l'attaquant a besoin d'identifier l'algorithme de cryptographie et notamment la clé secrète pour :

1. décoder l'information
2. comprendre sa signification
3. trouver les bits qu'il va devoir modifier
4. recoder les données pour les retransmettre sous la même forme au lecteur ou à la carte.

Cette attaque est très difficile à mettre en œuvre, car elle requiert beaucoup de technique et de moyens pour la réaliser. A ce jour, aucun article ne traite d'une réalisation pratique de cette attaque. Certains auteurs déclarent même qu'elle est impossible à mettre en place, mais pour de mauvaises raisons, car ils prennent un cas où la carte est proche du lecteur [HAS2006]. Le temps est un facteur important lors d'une telle attaque, car il est souvent nécessaire de démoduler le signal ; on peut aussi avoir besoin de décrypter le message et le réencrypter. Toutes ces étapes prennent du temps. Les normes RFID prévoient un temps de réponse jusqu'à 5 s, ce qui est largement suffisant pour faire n'importe quelles modifications dans les données.

Cette attaque peut aussi permettre de renforcer la force de l'attaque relai simple. Par exemple, elle peut être utilisée pour envoyer de manière aléatoire des bits lorsque le lecteur utilise un protocole de distance bounding pour détecter l'attaque relai.

5. Déni de service

A. Protocoles d'anticollision

Un protocole d'anticollision est un algorithme permettant d'éviter que plusieurs transpondeurs communiquent en même temps. En effet, si plusieurs transpondeurs répondent en même temps, le lecteur ne sera pas capable de décoder l'information. Dans les normes actuelles, on trouve principalement deux protocoles différents : un protocole déterministe et un protocole probabiliste. Ces deux protocoles peuvent être utilisés pour empêcher le lecteur d'accèder à la carte. Ainsi, ces solutions peuvent être utilisées pour faire du déni de service.

a. Protocole déterministe

Ce protocole permet de connaître le temps que va prendre la gestion des collisions en fonction du nombre de transpondeurs présents dans le champ magnétique généré par le lecteur. Cet algorithme se déroule en deux étapes.

La première consiste en une requête du lecteur ; il appelle dans un premier temps tous les transpondeurs présents dans son champ. Tous les transpondeurs présents répondent alors en même temps la même trame. Aucune collision ne se produit pendant cette étape.

Dans la seconde étape, le lecteur envoie une trame particulière comportant plusieurs informations importantes comme le nombre de bits valides contenus dans la trame (NVB), des bits correspondants à tout ou une partie de l'identifiant de la carte (UID CLn). L'objectif de cette requête est de réaliser une sélection dans les transpondeurs présents dans le champ du lecteur. Seuls les transpondeurs dont l'identifiant (UID) commence par l'UID CLn pourront répondre au lecteur.

Exemple avec trois transpondeurs dans le champ :

- Transpondeur 1 : 01100001 10010011 11001010 11110011
- Transpondeur 2 : 01101001 10100011 01011101 01101000
- Transpondeur 3 : 01100001 10010011 10110010 11101000

Pendant la première étape, le lecteur envoie une première requête pour laquelle les trois transpondeurs répondent en même temps.

Pendant la seconde étape, le lecteur envoie la trame d'anticollision en indiquant qu'il ne connaît aucun bit valide de l'UID. Les trois transpondeurs envoient alors leurs UIDs en même temps. Ces trois UID n'étant pas identiques, une collision se produit dès qu'un bit diffère entre les trois transpondeurs. La première collision se produit donc au niveau du $5^{ème}$ bit puisque le transpondeur 2 envoie un '1' et les transpondeurs 2 et 3 envoient '0'.

Le lecteur peut connaître la localisation de la collision lorsqu'il reçoit les réponses des transpondeurs ; il y a 4 bits valides dans l'exemple. Il renvoie alors une nouvelle trame d'anticollision en indiquant qu'il y a 4+1 bits valides, et il envoie ces 5 bits valides 0110 0. A ce niveau là, seuls les transpondeurs dont l'UID commence par 01100 pourront répondre au lecteur (c'est-à-dire les transpondeurs 1 et 3). Une nouvelle collision se produit au niveau du $2^{ème}$ bit du $3^{ème}$ octet.

Le lecteur localise la collision, il envoie de nouveau une trame d'anticollision en indiquant qu'il y a 18 bits valides soit 01100001 10010011 11. Seul le transpondeur 1 répond à cette requête puisque seul celui-ci a un UID commençant par ces bits.

Le lecteur peut alors sélectionner le transpondeur 1 puisqu'il connait son UID complet.

Il est possible d'utiliser cet algorithme pour développer un protocole bloquant. L'algorithme précédent est appelé tree-walking, voir la figure I-16, car on parcourt un arbre dont les feuilles sont les différents identifiants possibles pour le transpondeur.

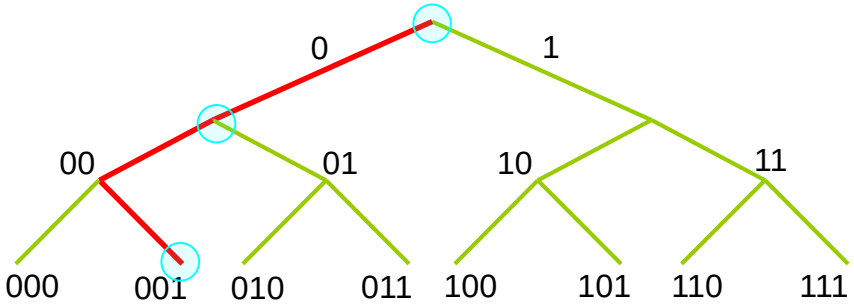


Figure I-16 – Tree Walking pour des UID de 3 bits

L'algorithme tree-walking utilise le principe du parcours d'arbre. Les différents nœuds correspondent aux éventuelles collisions qu'il peut y avoir. Pour un UID avec 3 bits, il y a 2^3 possibilités soit 8 tags avec des identifiants différents. L'objectif du protocole bloquant est de créer une collision à chaque nouvelle requête d'anticollision du lecteur pour empêcher le lecteur d'accéder aux UIDs des transpondeurs. Pour cela, un système permet d'envoyer un '0' et un '1' à chaque requête du lecteur. Un tel protocole est un déni de service, car il peut empêcher un vrai lecteur d'accéder à une carte.

b. Protocole probabiliste

Ce protocole permet d'éviter l'utilisation d'un protocole basé sur les collisions au niveau bit qui demande un codage précis et une bonne synchronisation. Ce protocole probabiliste est moins rapide que le précédent, car le temps d'identification pour x tags peut varier d'une séance d'identification à une autre. Il est appelé « méthode des times slots » ou bien méthode « Aloha ». Le principe est simple, chaque transpondeur doit répondre au lecteur dans des intervalles de temps déterminés.

Au début du premier round, le lecteur envoie le nombre de slots qui vont être utilisés. Chaque transpondeur doit répondre aléatoirement dans un de ces slots. Il y a deux possibilités :

- Lorsqu'un transpondeur répond seul dans un slot, le lecteur récupère son identifiant et le met de côté.
- Si deux transpondeurs répondent dans le même slot, il y a collision Le lecteur relance un round sans les transpondeurs qui ont répondu seul dans leur slot.

Au round suivant, moins de transpondeurs répondent, donc il y a plus de probabilité qu'il n'y ait pas deux réponses de transpondeur dans un même slot. S'il y a quand même une collision, le lecteur relance encore un round. Le lecteur lance des rounds jusqu'à qu'il ait enregistré tous les identifiants.

Il est possible d'utiliser cet algorithme pour développer un protocole bloquant. En effet, un attaquant peut se placer au milieu de tous les transpondeurs et répondre un identifiant aléatoire à chaque round dans chacun des times slots (figure I-17). Le lecteur va relancer un round car il y aura une collision dans chacun de ces slots. L'algorithme de collision peut alors durer éternellement.

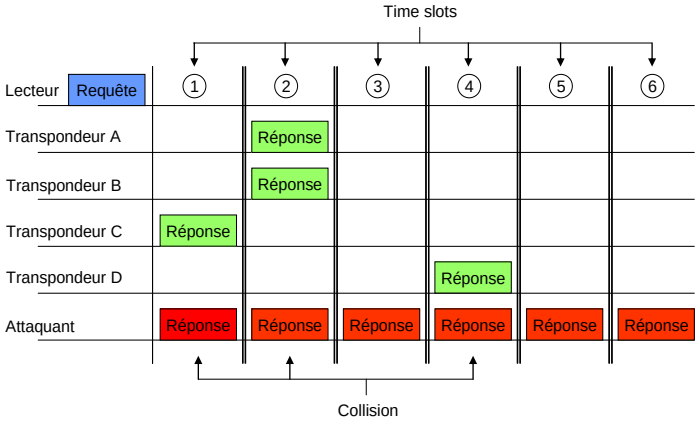


Figure I-17 – Protocole bloquant associé à la méthode Aloha

B. Brouillage

Cette attaque est assez simple à mettre en œuvre ; son objectif est de brouiller le signal du lecteur. L'attaquant doit émettre un champ magnétique dans la même bande de fréquence que le lecteur avec une bande passante au moins égale et un champ magnétique très important. La densité spectrale de puissance du signal généré par le brouilleur doit être supérieure à celle du système sans contact.

La puissance du champ émis par un lecteur est limitée par une norme européenne : la législation ETSI (figure I-18). La valeur du champ magnétique à 10 m ne doit pas dépasser 42dBµA/m.

Si l'attaquant développe un dispositif permettant d'obtenir un champ magnétique d'amplitude supérieure à celle imposée par la législation, il est sûr de brouiller le signal du lecteur. La puissance nécessaire pour brouiller un signal sans contact est faible (une puissance de 1 ou 2W est suffisante). Le brouillage du signal transpondeur est plus facile que celui du signal lecteur, car la modulation de charge de la carte possède un indice de modulation très faible. Le brouillage d'un système dépend principalement de la capacité de l'attaquant à générer un champ de forte amplitude. Cependant, malgré l'absence de littérature à ce sujet, on peut penser que la distance de brouillage est limitée à quelques dizaines de centimètres.

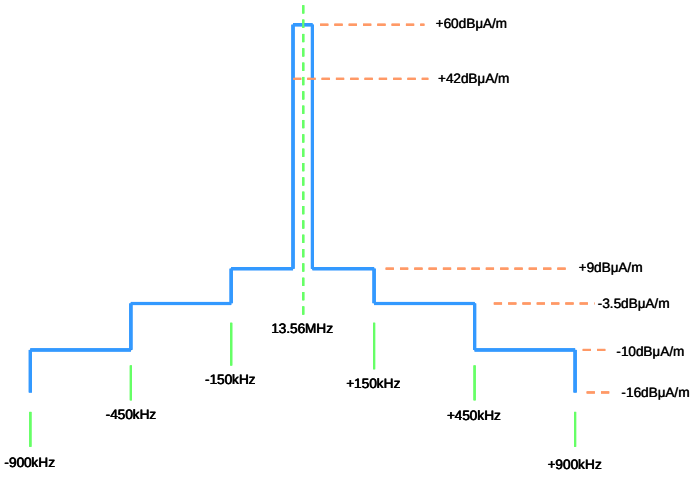


Figure I-18 – ETSI EN300-330 13.56 MHz : champ magnétique maximum à 10 m du lecteur

C. Blindage et cage de faraday

L'objectif d'un tel système est de contrôler l'émission et la réception de données ; il est possible de s'en servir pour faire du déni de service. Les ondes électromagnétiques peuvent être bloquées ou radicalement atténuées en utilisant un système de type cage de faraday. En plaçant une carte sans contact dans une feuille métallique, le lecteur ne peut plus communiquer avec celle-ci, car les ondes électromagnétiques traversent certaines épaisseurs de métal (celles-ci dépendant de la fréquence du système). Pour être efficace en HF, la feuille métallique doit être plus épaisse que 20 µm. Le métal peut être du cuivre ou de l'aluminium, voir la figure I-19. Cette solution peut être utilisée pour passer à côté de systèmes RFID EAS sans être inquiétée en entourant les produits non payés par une feuille métallique.

Figure I-19 – De tels systèmes bloquent les signaux dans la gamme de fréquences 10MHz-20GHz [DIRFwear, MobileCloak]

6. Attaque side-channels

Les attaques side-channels (fuite d'informations) sont des attaques basées sur la fuite d'informations de la puce. Elles consistent à espionner l'activité interne de la puce afin d'y déceler des secrets (clé secrète, algorithme de cryptage). Seule l'attaque RFA est spécifique au lien sans contact [CAR2005].

RFA (RadioFrequency Analysis) : Enregistrement du rayonnement électromagnétique émis en dehors des échanges par une carte sans contact au travers du canal normal c'est-à-dire par son antenne.

L'énergie dépensée par une carte sans contact provient directement du champ radiofréquence généré par le lecteur. Les fuites d'informations introduisent une modulation d'amplitude sur la porteuse à 13.56 MHz du lecteur. L'amplitude s(t) de cette modulation peut être décrite par l'équation I-1.

$$s(t) = (P_{const} + p(t)).\cos(w_{reader}.t) \qquad \text{(I-1)}$$

Avec Pconst l'alimentation constante de la puce et p(t) les variations introduites par l'exécution de différents processus, par exemple des protocoles cryptographiques.

L'article [KAS2009] présente un système analogique de démodulation spécialement étudié pour l'analyse des rayonnements électromagnétiques. Les auteurs ont démontré la puissance de leur système sur des cartes sans contacts du commerce. Leur attaque, voir la figure I-20, permet en quelques heures de retrouver la clé utilisée pour un 3-DES ou un AES (protocoles de cryptographie implémentés sur certains systèmes sans contact). Le circuit électronique développé permet d'isoler et d'amplifier les différentes fuites d'informations de la carte (figure I-21). Leur système nécessite la capture du champ RF avec une sonde de champ. L'analyse des différentes données montre de grosses faiblesses sur les systèmes existants, en particulier sur la carte Mifare DESFire.

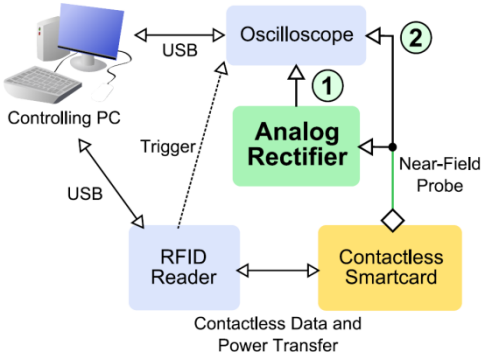


Figure I-20 – Système d'analyse complet

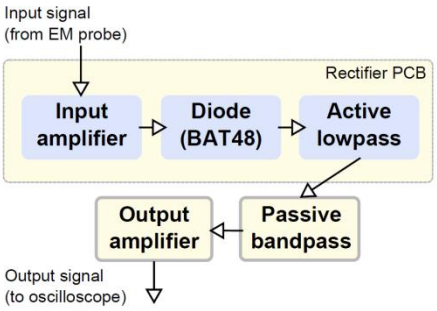


Figure I-21 – Système de démodulation analogique

7. Destruction par désactivation

A. Destruction par exposition à un champ magnétique important

Il est en effet possible de détruire un transpondeur en générant un fort champ magnétique que celui-ci ne pourra pas supporter. Cette attaque fonctionne principalement avec les transpondeurs à boucle inductive. Si la tension induite dans la bobine de l'antenne excède une certaine valeur, la puce peut être irrémédiablement détruite [FOI2004]. En général, un champ magnétique supérieur à 12 A/m suffit pour détruire une puce. Pour détruire un ou plusieurs transpondeurs en même temps en se plaçant à quelques mètres, le transmetteur devrait fournir une puissance considérable. L'attaque possède donc une distance de fonctionnement réduite.

De nombreux sites expliquent comment réaliser son propre destructeur de transpondeurs RFID. Le RFID zapper, voir la figure I-22, est un petit gadget permettant de détruire les puces RFID [ZAP2005]. Il génère un champ électromagnétique très puissant, mais de courte portée en utilisant l'électronique du flash d'un appareil photo. La puce RFID reçoit un choc similaire à une mini EMP (Electro Magnetic Pulse) qui grille ou désactive de façon permanente la puce RFID.

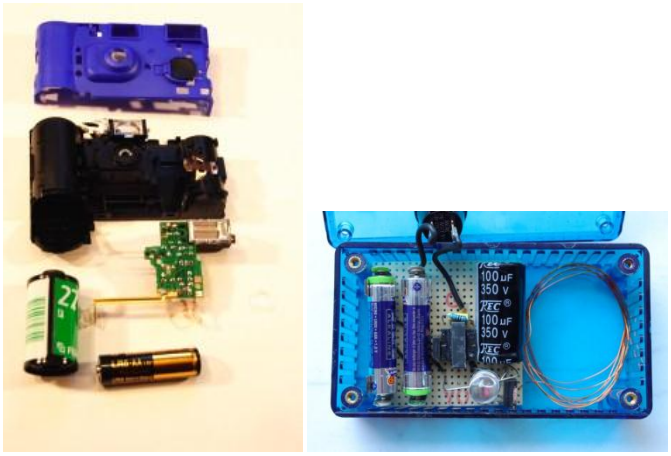


Figure I-22 – Réalisation d'un RFID zapper

On trouve une multitude de gadgets de cette sorte sur Internet avec les circuits électroniques permettant de faire son propre RFID zapper. Certains de ces appareils sont équipés de « radars » permettant de savoir s'il y a présence ou non de tags dans une zone.

B. La commande kill

Chaque transpondeur conforme à la norme EPC contient un code permettant d'effacer toutes les données contenues dans la puce [ISO18000-3]. Cette commande peut être utilisée à mauvais escient ; tout lecteur ou dispositif envoyant le signal de commande kill avec le bon mot de passe pourra détruire les données du transpondeur. Une simple requête non protégée d'un dispositif suffit pour obtenir ce mot de passe. En conclusion, n'importe quel attaquant peut effacer les données contenues sur un tag EPC.

C. Destruction chimique ou mécanique

Un transpondeur est généralement constitué d'une antenne et d'une puce ; ces deux éléments sont de simples pièces mécaniques. L'antenne est une simple bande de cuivre ; la puce est fragile et uniquement protégée par un boîtier plastique. Il existe de nombreuses solutions permettant de détruire un transpondeur. La majorité de ces solutions laisse des traces visibles des dommages et nécessite l'accès à la carte. L'antenne est très vulnérable ; un simple coup de ciseaux en travers du transpondeur permet de désactiver la puce, car l'antenne est nécessaire pour l'alimentation et la transmission de données. D'autres solutions permettent de ne donner aucun indice sur les dommages intentionnels [INS2008]. Couper délicatement à proximité de la puce ou frapper cette puce avec un marteau sont des possibilités lorsque la puce et l'antenne ne sont pas encapsulées dans du plastique. Il est aussi possible d'endommager la carte à l'aide de produits chimiques.

8. Substitution, clonage, replay

Ces trois attaques sont regroupées dans la même partie, car leurs principales caractéristiques sont les mêmes. Toutes ces attaques nécessitent la récupération malhonnête de données sur une autre carte sans contact. Ces attaques sont souvent précédées d'une attaque eavesdropping ou d'une attaque skimming permettant à l'attaquant de récupérer les données enregistrées dans la mémoire d'un transpondeur. Ces données peuvent alors être enregistrées sur un transpondeur vierge pour obtenir une copie de la carte précédemment attaquée. Ecrire des données sur une carte vierge est assez simple puisque l'on peut trouver sur internet tout le matériel permettant de programmer n'importe quelle carte utilisant un microprocesseur [DNS2007]. Un attaquant peut aussi utiliser la violence pour voler la carte sans contact d'une personne. Dans les deux cas précédents, l'attaquant possède une carte sans contact avec un nouveau UID et de nouvelles données. Ceci conduit aux trois attaques suivantes: substitution, clonage et attaque replay.

Par exemple, il est possible de remplacer un tag RFID sur un objet par le tag d'un autre objet moins coûteux ou avec un tag reprogrammé par le pirate. L'attaque replay consiste à envoyer à un lecteur ou une carte valide les séquences précédemment obtenues par eavesdropping ou skimming. Grunwald a montré sa capacité à cloner un passeport électronique pour se faire passer pour une autre personne ; un terroriste est donc capable de passer une frontière avec une fausse identité [ZET2006]. Cependant, les passeports actuels intègrent des protocoles d'authentifications ne permettant plus de réaliser ce type d'attaques.

PARTIE III. CONTRE-MESURES EXISTANTES

Cette partie est un aperçu des contre-mesures existantes pour réduire le manque de sécurité des communications sans contact. Les contre-mesures identifiées sont des solutions basées sur la couche physique de ces systèmes sans contact.

1. Brouillage actif

Ce principe a déjà été évoqué dans la section « Blindage et cage de faraday », un individu peut transporter un dispositif envoyant un champ radiofréquence assez fort et dans la même bande de fréquence que le système sans contact de façon à empêcher un lecteur d'accéder à la carte ou de comprendre sa réponse. Ce type de contre-mesure n'est pas vraiment légal puisqu'elle crée un déni de service et qu'elle peut détruire les systèmes sans contact à proximité si le signal de brouillage émis est de forte puissance.

2. Distance Bounding

Un protocole de distance bounding est un algorithme de cryptographie qui permet de définir une limite d'éloignement entre un émetteur et un récepteur qui communiquent ensemble.

Ce type de protocole est une des seules contre-mesures identifiées pour détecter les attaques relais. La résolution maximale obtenue à l'aide d'un signal de fréquence porteuse conforme aux normes des systèmes sans contact est de l'ordre du kilomètre. Il est donc nécessaire d'ajouter une nouvelle technologie de communication pour utiliser un tel protocole. Ces protocoles ont tout d'abord été introduits pour des systèmes filaires [BRA1993].

Dans [HAN2005-B], les auteurs proposent un tel protocole d'authentification basé sur la localisation de la carte. L'objectif est de vérifier que la carte est proche du lecteur. Cette contre-mesure utilise la technologie UWB qui permet de mesurer des distances avec une résolution inférieure à 30 cm. Cette solution propose un protocole d'authentification en trois phases :

- Une phase pour l'échange du secret (authentification classique)
- Une phase de questions-réponses très rapides pour mesurer le délai entre la question et la réponse
- Une phase de vérification et conclusion

Cette solution est assez difficile à mettre en œuvre puisque l'implémentation de l'UWB dans un système RFID ajoute un coût et une complexité non négligeables. De plus, le temps de propagation reste difficile à isoler car il est faible par rapport au temps de traitement et pas forcément constant.

Dans [REI2007], la solution consiste à mesurer le temps entre la fin de l'émission de la requête par l'émetteur et le début de la réponse du récepteur. Pour cela, l'auteur se base sur deux points de référence identifiés lors de changements d'état du signal. Ce système permet de mesurer des temps de communication précis à $1/(2*fc)=36.9\mu s$. Cette résolution est théoriquement suffisante pour détecter la plupart des attaques relais. Cependant, cette solution ne prend pas en compte certaines caractéristiques du système : la carte ne répond pas toujours au même moment, le temps de traitement du signal peut augmenter la durée du relais, l'attaquant peut de plus agir sur le relais pour rendre inefficace cette contre-mesure.

Munilla et al. proposent un protocole basé sur la norme ISO 14443-A, le lecteur module son champ en OOK de façon à générer de courtes séquences périodiques qui seront utilisées comme bits de synchronisation [MUN2008]. Entre deux bits de synchronisation, le lecteur active son champ RF de manière à alimenter la carte et lui permettre de répondre. La carte peut donc moduler le champ du lecteur de façon à indiquer sa réponse, l'amplitude du champ résultant permet l'identification de la valeur du bit envoyé par la carte. Pour mesurer le délai entre la requête et la réponse de la carte, le lecteur compte le nombre d'échantillons entre le retournement du champ RF et le moment où celui-ci devient stable. Ce temps donne une bonne indication sur le délai introduit par le relais. Les auteurs concluent que leur solution peut détecter des attaques relais simples avec des délais inférieurs à 1 µs mais qu'elle est inefficace contre les attaques de type « distance fraud attack" » Cette solution impose une modification des normes sans contact actuelles. De plus, le champ RF est souvent inactif, la carte risque de ne plus être alimentée.

De nombreux auteurs ont ensuite proposé des variantes proches de la solution de G Hancke et M. Kuhn. D'autres articles proposent d'autres protocoles « distance bounding » ou des attaques contre ces mêmes protocoles [HAN2008-B, KIM2008, MIT2010, MUN2010, TU2007].

3. Déni de service

La littérature donne de nombreux exemples de solutions permettant à l'individu de désactiver sa carte de façon temporaire.

La solution la plus simple est un portefeuille se comportant comme une cage de faraday de façon à se prémunir contre l'activation de sa carte contre son gré. Cette cage de faraday empêche les ondes radiofréquences de passer en travers et donc d'activer une carte placée à l'intérieur. Un inconvénient de ce type de contre-mesures est que l'on ne peut pas placer de gros objets dans une cage de faraday, cette contre-mesure est plus adaptée aux cartes format ID1 (cartes de paiement)

Dans [KAR2005], l'auteur présente des structures physiques permettant à l'individu de désactiver sa carte en séparant de façon temporaire ou définitive la puce de l'antenne. Il propose 3 solutions différentes :

- Le conducteur électrique reliant l'antenne à la puce peut être détachable
- Il est possible de perforer l'antenne
- L'antenne peut être complètement enlevée

Ces solutions peuvent permettre une réactivation du tag par la suite. Il est cependant fastidieux d'enlever toutes les antennes si on achète un chariot complet de marchandises taguées.

4. Ajout de bruit

Pour lutter contre l'attaque eavesdropping, plusieurs solutions utilisant l'ajout de bruit ont été développées.

A. Tag bruité

En 2006, C. Castelluccia et G. Avoine proposent une solution nommée « noisy tag » [CAS2006]. L'objectif est de générer du bruit dans le canal de communication pour créer un canal de communication sécurisé et empêcher un attaquant d'espionner la communication. Pour cette contre-mesure, un tag bruyant est placé à proximité du lecteur. Il va permettre d'échanger une clé secrète entre le lecteur et le tag de façon sécurisé. Pour cela, le tag bruyant injecte un bruit dans le canal, le tag peut soustraire ce bruit, mais pas l'espion. Le principe est le suivant :

1. Le tag bruyant génère une séquence de bits aléatoires : le bruit N(i)
2. Au même moment, le lecteur envoie les bits de la clé secrète
3. Un espion verra k(i) + N(i)
4. Le tag, en soustrayant le bruit N(i) retrouve k(i)

Les auteurs proposent trois protocoles différents utilisant ce principe.

Plusieurs inconvénients peuvent être identifiés. Tout d'abord, l'échange d'une clé secrète impose une modification des normes ISO. Ensuite, le bruit injecté est numérique ; les signaux du tag et ceux du tag bruyant n'ont pas vraiment les même amplitudes ce qui rend la détection des signaux plus faciles

B. Lecteur bruité

Dans [SAV2007], une équipe de chercheurs du CEA propose une autre solution permettant d'utiliser le bruit pour assurer la sécurité de la communication sans contact, voir la figure I-23. Le bruit utilisé dans cette proposition est un bruit aléatoire et analogique, il est dans la même bande passante que la communication. Il doit aussi être synchrone avec la réponse de la carte. Le lecteur génère donc ce bruit pendant la réponse de la carte car c'est cette phase qui contient le plus

d'informations secrètes. Le lecteur connait le bruit qu'il a envoyé, il peut donc le soustraire au signal reçu lors de la phase de réception, il retrouve ainsi le message de la carte.

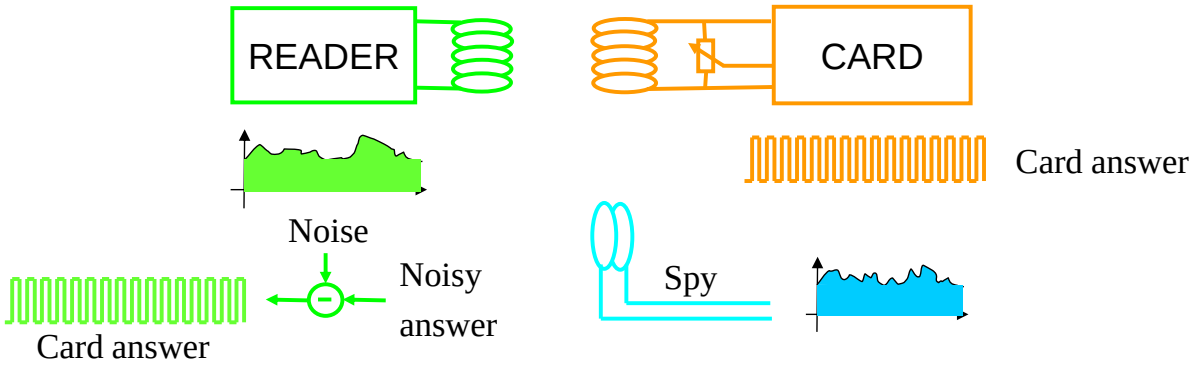


Figure I-23 – Système complet avec une sonde espion

La même année, G. Hancke propose une solution assez proche, la carte module sa réponse sur la porteuse bruitée du lecteur [HAN2007].

5. Protocole bloquant

A. RFID guardian

Le RFID Guardian est un dispositif électronique utilisé par des personnes possédant des transpondeurs RFID [RIE2005-A, RIE2005-B, RIE2006, RIE2008]. Cet outil propose plusieurs fonctionnalités :

- L'écoute de l'activité RFID autour de l'individu, l'enregistrement et l'affichage des tags en possession de son utilisateur
- Le scan des tags dans la zone
- La gestion de clés secrètes
- Le blocage des lecteurs non autorisés

Lorsqu'un lecteur envoie une requête à l'un des tags du propriétaire du RFID Guardian, le dispositif va vérifier que la requête est permise. Si cette requête n'est pas permise ou que le lecteur n'est pas authentifié, alors le dispositif brouille le signal envoyé par le tag lors de sa phase de réponse. Le dispositif propose aussi une ACL (Access Control List) qui permet à l'utilisateur de choisir les requêtes que les tags doivent acceptées en fonction du lieu, des tags, des lecteurs et de la requête. Le brouillage utilisé par le dispositif est actif et aléatoire. Le dispositif RFID Guardian possède de nombreuses fonctionnalités permettant de rassurer l'individu sur la sécurité de sa vie privée ; il est très complet.

B. Blocker tag

Le « blocker tag » est un transpondeur intelligent permettant de bloquer les tags sélectionnés en utilisant les algorithmes d'anticollision de l'ISO14443-A [JUE2003]. La partie sur les algorithmes bloquants explique le principe utilisé par le « blocker tag » pour empêcher le lecteur de comprendre les réponses du transpondeur. Pour cela, il simule tous les identifiants de tags possibles et crée ainsi des collisions. Le lecteur va alors explorer tout l'arbre, soit 2^{64} possibilités. Le principal inconvénient de cette méthode est que le blocker tag n'est pas sélectif et que tous les tags sont bloqués, un tel dispositif relève du déni de service.

C. Autres solutions basées sur les protocoles bloquants

On trouve de nombreux articles proposant des solutions proches du RFID Guardian pour sécuriser la communication RFID.

Dans [DIM2008], l'auteur propose un proxy qui permet à son propriétaire de choisir comment les tags envoient des infos. Il est ainsi possible de modifier l'identité du tag ou de masquer ces réponses.

Dans [JUE2003], l'article décrit une solution appelée REP (RFID Enhancer Privacy) qui permet de prendre l'identité et les données d'un tag pour ensuite le simuler lors d'une communication avec un lecteur. Le REP possède une plus grosse puissance de calcul qu'un tag ; il peut donc utiliser des systèmes de sécurité plus complexes.

Dans [KIM2006], les auteurs ont développé un dispositif mobile, le MARP (Mobile Agent For RFID Privacy protection) permettant d'améliorer la protection de la vie privée. Ce dispositif permet d'obtenir un plus haut niveau de sécurité, car il possède une unité de calcul plus puissante qu'un tag. Le MARP acquiert les secrets du tag, met ce tag en mode « sleep » et le remplace lors de communications RFID. Les lecteurs communiquent donc avec le MARP au lieu du tag.

On trouve d'autres articles sur ce sujet, on peut citer par exemple [JUE2004] qui propose une version software du tag bloquant.

6. Ajout d'un canal

Certains auteurs proposent la mise en place d'un deuxième canal de communication pour sécuriser la couche physique des systèmes sans contact.

Dans [JUE2004], l'auteur décrit une méthode pour éviter la contrefaçon de billets et leur utilisation dans des transactions criminelles. L'insertion de tags dans les billets de banque de forte valeur permettrait de tracer les billets et d'éviter ainsi les contrefaçons. Le principal inconvénient de cette méthode est qu'il est possible de connaître les billets qu'elle a en sa possession avec un faux lecteur, ce qui peut encourager un vol. A. Juels et R. Pappu proposent d'ajouter un accès au transpondeur RFID par canal optique pour diminuer la distance de communication entre le lecteur et la carte.

Dans [LEH2006], les auteurs montrent comment il est possible d'améliorer la sécurité des communications sans contacts en combinant RFID et mémoires optiques, voir la figure I-24. Une mémoire optique peut être un hologramme ou un code-barre par exemple, le lecteur et le transpondeur contenant la mémoire optique doivent être en ligne de vue directe ce qui rend l'écoute et le skimming plus difficiles. Ce canal de communication optique peut permettre d'envoyer des clés secrètes….

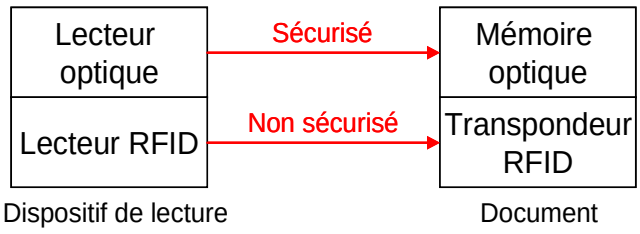


Figure I-24 – Système combinant RFID et mémoire optique

7. Ajout d'une technologie

Dans [YU2006], les auteurs proposent l'utilisation de la technologie UWB afin d'améliorer la sécurité des systèmes RFID. Les avantages de l'UWB sont en faveur d'une telle solution :

- Communication plus difficile à espionner, car la bande passante est très large

- Possibilité d'utiliser des cryptogrammes simples
- Faible latence
- Plus résistante aux interférences

Un tel système est cependant plus complexe pour un simple tag RFID puisque l'on devra ajouter en plus du front-end classique un front-end RFID. Une telle modification du tag entraine donc aussi un surcoût non négligeable pour un tag.

8. Interrupteurs commandés

Plusieurs solutions ont été développées pour permettre à l'utilisateur de cette technologie de pouvoir activer sa carte sans contact uniquement avec son consentement. L'objectif est de lutter contre toutes les attaques basées sur l'activation d'une carte sans contact par un lecteur malveillant (skimming et attaque relais). La solution la plus adaptée pour ce type d'attaques est l'interrupteur.

A. Interrupteur élastomère résistif [BIE2007]

L'interrupteur développé par les auteurs du brevet US2007/0290051 est positionné entre deux tronçons de l'antenne inductive reliée à la puce sans contact (figure I-25). Le propriétaire de la carte peut réunir les deux parties de l'antenne par simple pression au niveau de l'interrupteur ; l'antenne est alors fonctionnelle et la carte peut être activée par un lecteur à proximité. L'interrupteur est séparé de l'antenne par un matériau élastomère résistif (figure I-26).

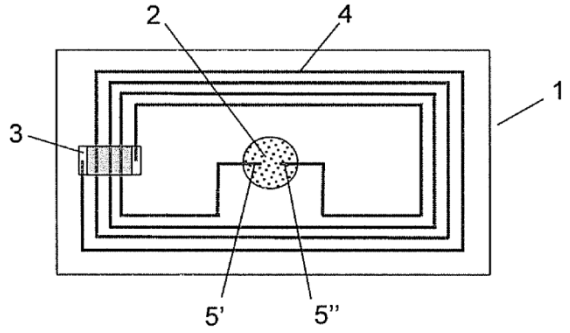


Figure I-25 – Interrupteur élastomère résistif (vue de dessous)

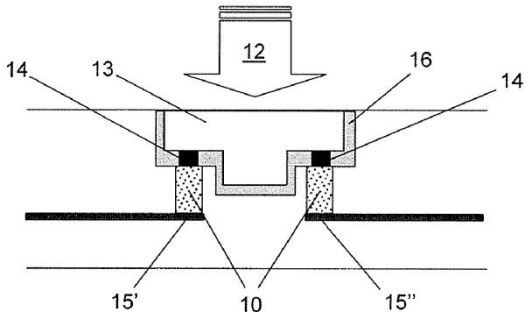


Figure I-26 – Interrupteur élastomère résistif (vue en coupe)

B. Interrupteur capacitif [GIE2002]

L'objet de cette invention est un interrupteur capacitif permettant d'autoriser l'activation de la carte par son propriétaire (figure I-27). Le système utilise la capacité des doigts de l'utilisateur pour activer une structure capacitive ; la carte détecte la variation de capacités à ses bornes et peut autoriser la communication.

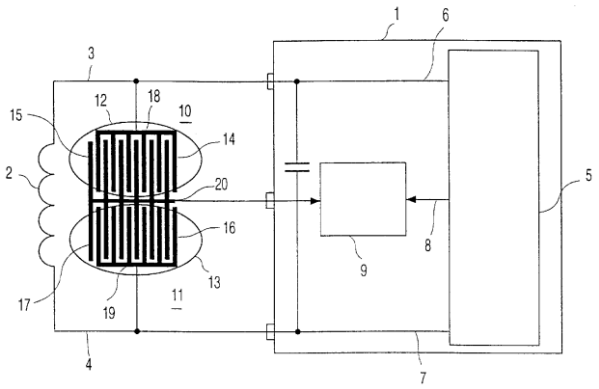


Figure I-27 – Système capacitif utilisé comme interrupteur

C. Capteurs de contrainte [LAR1994]

Les auteurs de ce brevet proposent une solution basée sur l'utilisation d'un capteur placé sur la carte sans contact et permettant de fournir une grandeur physique qui varie lors d'une action manuelle volontaire. Ce capteur peut être une jauge de contrainte détectant la flexion manuelle du plastique de la carte sans contact. Ce capteur peut aussi être une résistance thermique permettant de détecter la chaleur des doigts du propriétaire de la carte. D'autres solutions sont l'utilisation d'un thermocouple ou la mesure de la résistivité du doigt placé entre deux électrodes.

9. Modifications des antennes

A. Doubles antennes à interrupteurs [FIN2008]

Dans ce brevet, la carte est de format ID1. Son domaine d'application est toujours l'ISO14443. Elle possède deux antennes de taille, nombre de tours et facteurs de qualité différents. La première antenne est connectée à la puce et réglée à une fréquence très haute (relativement au 13,56 MHz), comme par exemple 50 MHz avec un facteur de qualité de 28, et une inductance propre très basse proche de 330 nH. Comme l'antenne a une fréquence de résonance très haute, elle ne récupère pas le champ pour alimenter la puce RFID et ne permet pas la transmission de données.

La deuxième antenne résonne à 14.5 MHz et possède un facteur de qualité de 70, avec une inductance propre d'environ 6 μH.

Un interrupteur et une capacité sont en série avec cette deuxième antenne. Quand l'interrupteur est fermé, les deux antennes sont couplées et la résonance est proche de 13.56 MHz. En fait, l'interaction de l'antenne à 50 MHz avec l'antenne à 14.5 MHz induit une fréquence de résonance globale proche de 13.56 MHz. Cette sécurité empêchera une attaque du type skimming, puisque l'utilisateur doit activer l'interrupteur pour pouvoir utiliser la carte.

B. Modulation d'espace limité [SER2002]

Ce brevet a pour objectif d'améliorer la sécurité des systèmes sans contact, en particulier contre l'attaque skimming et eavesdropping. Pour leurs auteurs, le manque de sécurité de ces systèmes est principalement introduit par le couplage électromagnétique entre le lecteur et la carte. Le brevet propose comme solution le remplacement des antennes lecteur et carte. Ils introduisent le concept d'antennes à double boucles inductives. Dans chacune de ces bobines, le lecteur injecte un signal en opposition de phase par rapport à celui de la boucle voisine. Lorsqu'on s'éloigne de l'antenne du lecteur, les deux signaux émis par les deux boucles interférent et s'annulent. Lorsque l'antenne de la carte est assez proche du lecteur, les deux signaux du

lecteur peuvent être récupérés sur chacune des boucles de la carte et sommés. Les auteurs appellent ce principe «modulation d'espace limité».

C. Antenne double-huit

Des antennes sécurisées ont été développées dans le cadre d'un DRT (Diplôme de recherche technologique) par Ricardo Malherbi-Martins [MAL2010]. L'objectif principal de cette étude était de développer un design d'antennes permettant la sécurisation du lien sans contact.

Une des principales attaques visées par cette contre-mesure est le skimming, une attaque qui consiste à activer une carte sans contact à l'insu de son propriétaire. Une possibilité pour contrer cette attaque est de réduire le couplage et donc la mutuelle inductance entre l'antenne du pirate et celle de la carte sans contact. Cette solution peut être réalisée en modifiant le design des antennes utilisées dans les systèmes sans contact actuels. Le principe de la solution développée est une antenne à deux bobines connectées de façon à générer un champ magnétique avec une différence de phase égale à π entre chaque bobine. Le champ magnétique ainsi créé possède des lignes de champ magnétique qui se superposent dans une zone, que nous appelons zone de communication et qui est située dans la partie centrale de l'antenne. En dehors de cette région, le champ magnétique est atténué. Un lecteur classique ne peut pas activer une carte intégrant une antenne à deux boucles (que nous appellerons antenne simple huit) car le courant s'annule au niveau de cette antenne (figure I-28). Si l'antenne du lecteur et celle de la carte sont basées sur le même design, le lecteur peut communiquer avec la carte mais avec une distance d'activation réduite (figure I-29). L'attaquant ne peut donc pas réaliser une lecture à distance d'une carte sans contact utilisant ce design d'antennes (figure I-30).

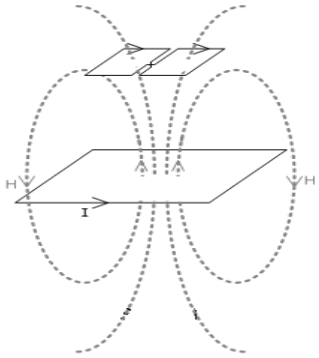


Figure I-28 – Scénario 1 : Lecteur standard et carte simple huit

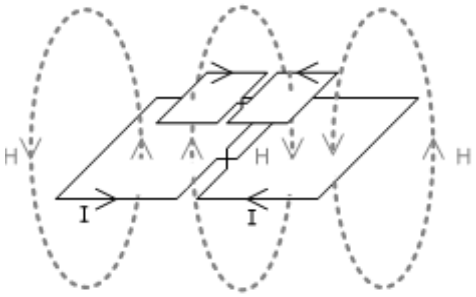


Figure I-29 – Scénario 2 : Lecteur avec antenne simple-huit et carte simple huit pour un couplage important

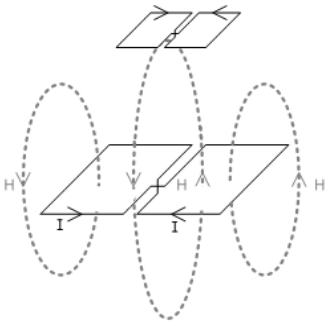


Figure I-30 – Scénario 3 : Lecteur avec antenne simple-huit et carte simple huit pour un couplage faible

Un second modèle a été développé utilisant quatre boucles au lieu de deux et appelé antenne double huit ou antenne trèfle (figure I-31 et I-32). Le principal avantage de ce nouveau design est la réduction du champ d'attaquant d'un pirate. En effet, cette antenne exige du pirate, en plus d'une distance d'activation réduite, un positionnement très précis d'une antenne par rapport à l'autre. Le principe est toujours le même ; chaque boucle possède une différence de phase de π par rapport à la boucle voisine

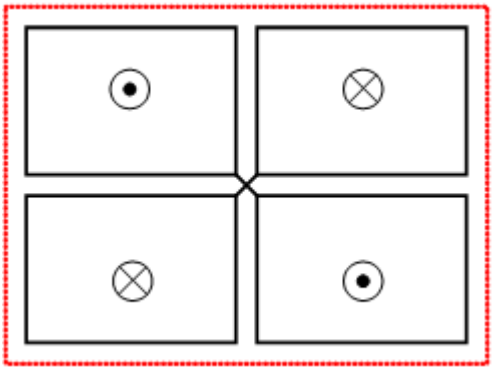


Figure I-31 – L'antenne double-Huit

Figure I-32 – PCB de l'antenne double-huit

10. Utilisation du canal sans contact

L'étude réalisée par Danev & al. en 2009 a été une des premières à démontrer que la couche physique des systèmes sans contact à 13.56 MHz pouvait être utilisée pour identifier une carte sans contact [DAN2009]. Pour cette étude, 4 expérimentations différentes ont été exécutées avec un matériel d'analyse spécifique. Les auteurs utilisent un lecteur sans contact standard et testent 50 cartes sans contact identiques et 8 passeports sans contact de 3 pays différents. L'antenne d'analyse est placée entre l'antenne du lecteur et l'antenne de la carte pour obtenir un couplage fort entre les différentes antennes et une forte influence de la carte (figure I-33).

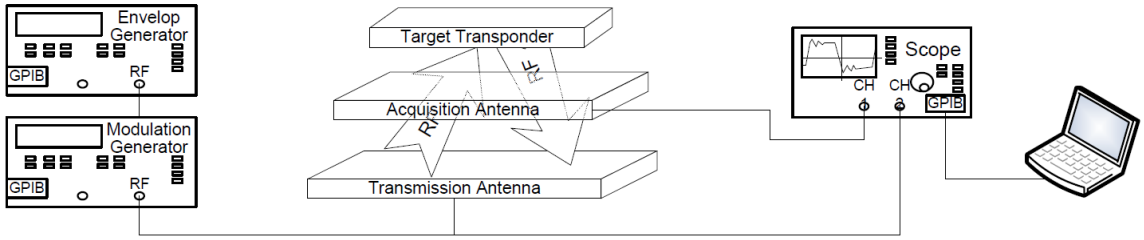


Figure I-33 – Système d'analyse des empreintes physiques

La première expérimentation consiste à enregistrer la requête et la réponse d'un système sans contact. Le lecteur active un champ radiofréquence à 13.56MHz, la fréquence utilisée dans les systèmes sans contact classiques. Cette étude permet de savoir si la carte répond différemment pour différentes cartes.

La deuxième expérimentation est très proche de la première. La seule différence est une fréquence porteuse de signal en dehors des spécifications de la norme. Les fréquences utilisées sont comprises entre 12.96 et 14.36 MHz. L'objectif est d'observer de plus importantes variations dans la réponse de la carte selon le fondeur de la puce.

La troisième expérimentation a pour objectif de tester les différentes cartes sous la contrainte de poussées d'énergie très rapides (energy burst). L'objectif est toujours de détecter des comportements liés à l'utilisation de signaux en dehors des spécifications données par la norme.

La dernière expérimentation consiste à observer l'influence de la carte sur un signal non modulé balayant la plage de fréquences 100 Hz à 15 MHz. L'objectif est de vérifier l'impact de chacune de ces fréquences sur les cartes sans contact et d'identifier les différences entre elles.

A partir de ces différentes expérimentations, les auteurs ont développé une série d'analyse permettant d'extraire une empreinte physique pour chaque carte sans contact. Leur étude est basée sur l'enveloppe et les propriétés spectrales des différentes réponses obtenues. Leur solution permet de différencier deux cartes sans contact «identiques» avec un taux d'erreur proche de 3

%. Il est aussi possible de classifier les cartes sans contact par fabricants et par pays avec un taux d'erreur nul. Cette technique peut être utilisée pour la détection de contrefaçons par exemple.

Chapitre II. Réalisation d'attaques

Introduction du chapitre

Les quatre principales attaques au niveau de la couche physique des systèmes sans contact sont l'eavesdropping, le skimming, l'attaque relais et l'attaque par déni de service. Toutes ces attaques ont été introduites dans le chapitre « Etat de l'art ». Cette partie présente l'analyse et la réalisation de deux de ces attaques : l'attaque eavesdropping et l'attaque relais. L'objectif n'est pas de montrer à un attaquant les moyens à mettre en œuvre pour frauder, mais plutôt de définir les caractéristiques principales de ces attaques de façon à identifier les contre-mesures les plus fiables par la suite.

PARTIE I. L'EAVESDROPPING (ECOUTE A DISTANCE)

Cette partie du rapport présente les travaux réalisés sur l'attaque eavesdropping, c'est-à-dire l'espionnage d'une communication standard entre un lecteur et une carte. Cette partie sera principalement consacrée à la réalisation d'expériences visant à montrer les faiblesses d'un système sans contact vis-à-vis d'une telle attaque.

Dans une première partie, une étude théorique sur les deux positions de Gauss et sur les données importantes échangées entre le lecteur et la carte sera présentée.

Dans une deuxième partie, nous étudierons les moyens à mettre en œuvre pour réaliser une telle attaque de façon à obtenir les principales caractéristiques.

Enfin, nous présenterons les résultats obtenus dans différentes conditions de mesures.

1. Théorie

A. Position de Gauss

La position de l'antenne de l'attaquant par rapport à celle du lecteur sans contact peut avoir un effet important sur la distance maximale à laquelle peut se placer cet attaquant. Lorsque le diamètre de l'antenne d'émission est considéré très inférieur à la distance antenne-point d'observation, l'antenne d'émission peut être vue comme un dipôle magnétique, voir la figure II.1.

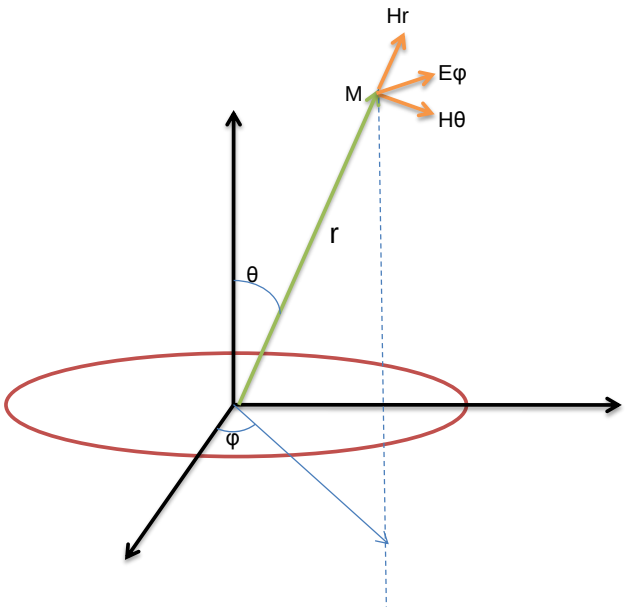


Figure II.1 – Champ électromagnétique à une distance r de l'antenne d'émission

Les équations II.1, II.2 et II.3 décrivent les formes des signaux électromagnétiques à une distance r du point d'émission.

$$H_\theta = \frac{I.S.\sin\theta}{4\pi r^3}(1 + j\frac{2\pi r}{\lambda} - \frac{4\pi^2 r^2}{\lambda^2})e^{j(wt2\pi r/\lambda)} \quad \text{(II.1)}$$

$$H_\varphi = \frac{I.S.\cos\theta}{2\pi r^3}(1 + j\frac{2\pi r}{\lambda})e^{j(wt2\pi r/\lambda)} \quad \text{(II.2)}$$

$$E_\varphi = j\pi\frac{I.S.\sin\theta}{w\varepsilon_0\lambda^2 r^2}(1 + j\frac{2\pi r}{\lambda})e^{j(wt2\pi r/\lambda)} \quad \text{(II.3)}$$

Avec I le courant dans l'antenne, S la surface de l'antenne d'émission, r la distance entre le point d'observation et l'antenne d'émission, λ la longueur d'onde du signal, et ω la pulsation de notre signal.

Soit θ l'angle entre l'axe du point d'observation au centre de l'antenne et la surface de l'antenne, on définit que θ=0° comme première position de Gauss et θ=90° comme deuxième position de Gauss.

En représentant l'amplitude du champ magnétique en fonction de la distance pour ces deux positions sous Matlab dans le cas d'une antenne d'émission ISO (diamètre de l'antenne=14.5cm) et I = 1A, on obtient les courbes de la figure II.2.

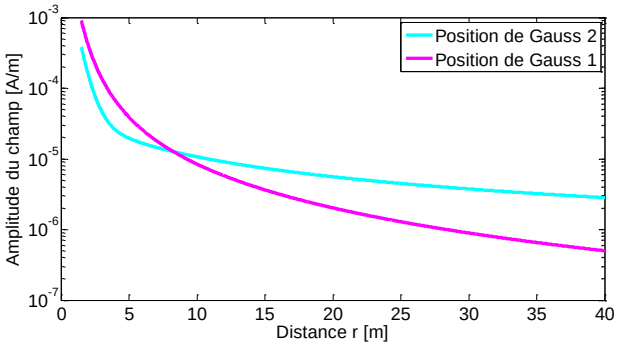


Figure II.2 – Amplitude de champ en fonction de la distance pour les deux positions de Gauss (échelle logarithmique)

La figure II.2 montre qu'avant une dizaine de mètres, l'amplitude du champ magnétique est supérieure dans la première position de Gauss. Après cette distance de 10 mètres, c'est dans la seconde position de Gauss que le champ magnétique est le plus grand.

La figure II.3 présente la position des antennes d'émission et de réception dans les cas des deux positions de Gauss. L'espion doit judicieusement placer son antenne par rapport à celle du lecteur (et non celle de la carte).

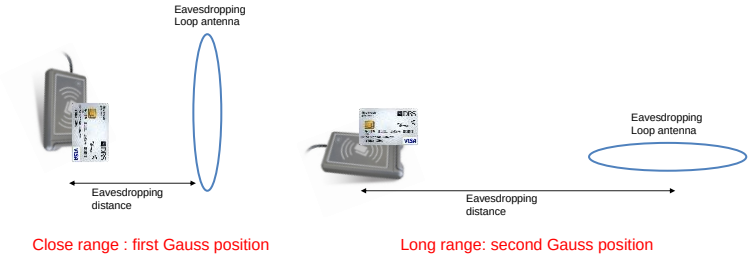


Figure II.3 – Positions des antennes pour les deux positions de Gauss

B. Données sensibles échangées

Les normes ISO14443-A et ISO14443-B, et notamment les sections 3 et 4, spécifient les données échangées entre le lecteur et la carte avant un possible protocole d'identification. Ces données ne sont pas toutes sensibles, mais certaines peuvent donner des informations privées permettant de faciliter une attaque ou des informations sur la carte sans contact. Il faut savoir que ces normes ont été écrites avec pour objectif principal la fiabilité de la technologie sans contact. Il existe dans les normes actuelles de grosses faiblesses au niveau de la sécurité que ce soit des données confidentielles échangées ou de faibles contraintes temporelles (faiblesses utilisées par les attaques relais). En général, les normes de communication n'ont pas pour vocation première la sécurité des systèmes.

Les systèmes sans contact échangent des informations sur les caractéristiques des signaux qu'ils vont envoyer telles que le débit, les temps de réponse et la longueur de trame. L'identifiant ou un identifiant provisoire est aussi envoyé, en particulier durant le protocole d'anticollision du lecteur. Ce protocole est surtout critique dans la norme ISO14443-A puisque l'identifiant de la carte (donnée particulièrement confidentielle) est envoyé plusieurs fois de la carte au lecteur et inversement.

2. Eavesdropping et moyens à mettre en œuvre

L'attaque eavesdropping est une attaque simple à réaliser puisqu'une simple bobine reliée à un oscilloscope permet déjà de récupérer le champ émis par un lecteur. Cependant, certaines « améliorations » peuvent permettre de rendre cette attaque plus dangereuse.

Nous nous intéressons ici uniquement aux cartes sans contact. Pour ces standards, la communication entre le lecteur et la carte s'établit à une distance très faible, de l'ordre de la dizaine de centimètres dans le cas de l'ISO14443 et de quelques dizaines de centimètres dans le cas de l'ISO15693. On peut donc imaginer que l'ordre de grandeur d'écoute d'une telle communication est proche du mètre. Les différentes études menées sur le sujet, théoriques mais aussi pratiques, ont montré que cette distance d'écoute pouvait être d'un mètre à plusieurs dizaines de mètres.

La figure II.4 présente la chaîne de mesure utilisée lors des mesures d'eavesdropping.

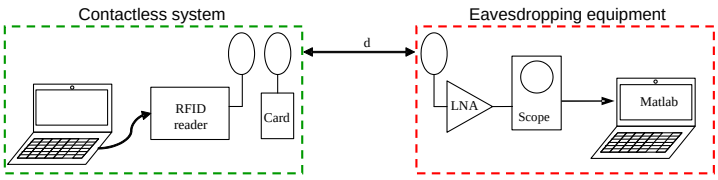


Figure II.4 – Chaîne de mesure pour l'eavesdropping

La station de base commande le lecteur sans contact connecté à une antenne conforme à la norme ISO10373, de diamètre 15 cm et de coefficient de qualité 10. Le lecteur émet un champ de 3.1 A/m mesuré à l'aide d'une bobine de calibration.

La carte sans contact est conforme à la norme ISO14443-A ou B selon les tests réalisés.

L'antenne de réception est placée à une distance « d » du système sans contact ; 3 antennes différentes ont été utilisées. La première antenne est identique à l'antenne d'émission ; c'est une antenne conforme à la norme ISO10373-6. Les deux autres antennes ont été réalisées par Thierry Thomas, ingénieur chercheur au CEA-Léti. Ces deux antennes ne sont pas adaptées 50 Ω car il est plus important de privilégier le facteur de qualité de l'antenne et un bruit minimal. L'anneau résonnant est formé par une boucle circulaire de câble coaxial d'un diamètre D (de 20 cm à 1 m). Les antennes sont choisies pour résonner à la fréquence 13.56 MHz pour privilégier l'écoute de la voie montante (requêtes du lecteur) et 14.4 MHz pour privilégier l'écoute de la voie descendante (réponses de la carte).

Un système analogique de traitement, en partie constitué d'un amplificateur faibles signaux et d'un filtre passe-bande centré à 13.56 MHz, est connecté d'une part à l'antenne et de l'autre à un oscilloscope qui va permettre de visualiser et d'enregistrer les signaux.

Les signaux enregistrés sont ensuite traités sous Matlab. La figure II.5 présente le système de démodulation implémenté sous Matlab. Le signal enregistré sur l'oscilloscope est analysé de façon à récupérer la fréquence de la porteuse de façon très précise. Ce signal d'horloge permet de démoduler le signal de manière synchrone de façon à identifier le signal du lecteur. Après cette première démodulation, il est possible de trouver le signal de la carte en identifiant de manière précise la fréquence de la sous-porteuse et en mélangeant le signal enregistré avec une sinusoïde à la fréquence trouvée.

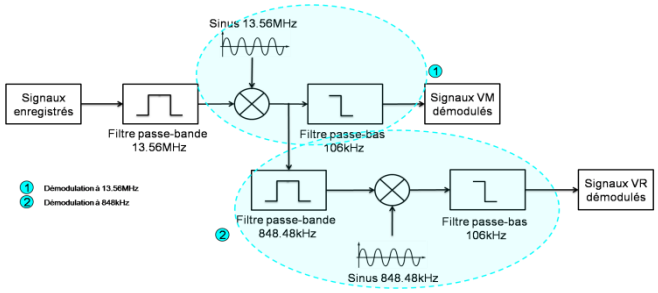


Figure II.5 – Synoptique du fichier de traitement Matlab

3. Expérimentation

A. Test à la MMNT

Ces tests ont été réalisés à la MMNT (Maison des Micro-Nano Technologies), une grande salle permettant de réaliser nos expériences dans un endroit moins perturbé par l'environnement et l'architecture du bâtiment.

La figure II.6 montre un plan de la salle et la disposition de notre système sans contact et notre système d'écoute.

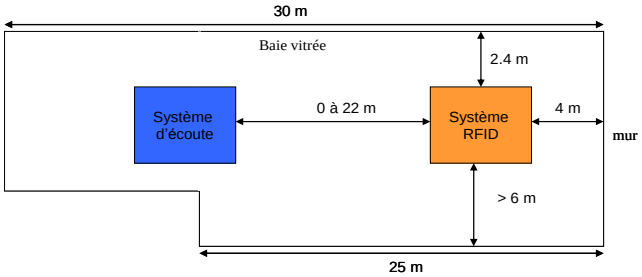


Figure II.6 – Plan du lieu de l'expérience

La figure II.7 présente des photos de l'expérience à la MMNT. On peut voir sur ces images le système sans contact placé sur le trépied et l'antenne espion fixée sur une planche en bois. Cette antenne est reliée au circuit de traitement analogique et à l'oscilloscope. Toute la chaîne de réception est alimentée par des batteries pour ne pas récupérer le signal espionné par des câbles d'alimentation.

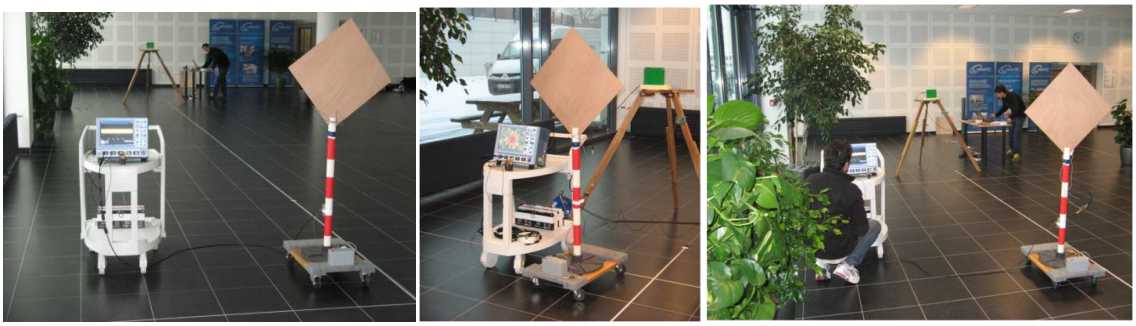


Figure II.7 – Photos de l'expérience

B. Amplitude des signaux

L'amplitude maximale des signaux est relevée tous les 4 m pour les différentes normes et les différentes antennes de réception pour la voie montante, à savoir l'antenne ISO et l'antenne coaxiale centrée en 13.56 MHz. Les figures II.8 et II.9 sont les courbes correspondant aux différentes amplitudes pour les différentes distances en position de Gauss 1 et 2

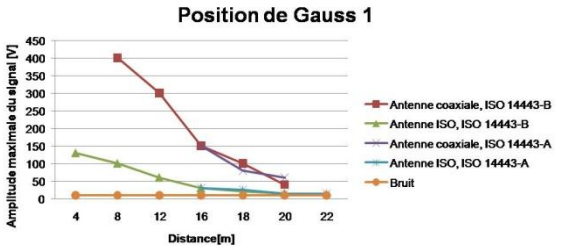


Figure II.8 – Amplitude des signaux enregistrés en première position de Gauss

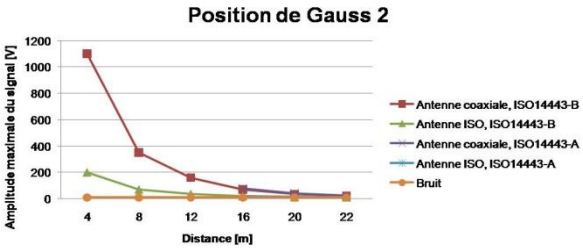


Figure II.9 – Amplitude des signaux enregistrés en deuxième position de Gauss

On ne retrouve pas les courbes prévues par la théorie ; la chaine de mesure semble introduire des modifications différentes sur l'amplitude du signal selon sa puissance et la structure métallique du bâtiment peut modifier le comportement du champ RF. Cependant, la décroissance de l'amplitude du signal (image du champ RF) correspond bien à la théorie.

a. Résultats de la voie montante

Les figures II.10-II.17 correspondent aux signaux enregistrés au niveau de la voie montante pour différentes normes, distances, positions de Gauss et antennes. Pour chaque figure, on trouve le signal enregistré sur l'oscilloscope, le signal démodulé et le signal remis en forme tel un signal binaire. Les signaux récupérés dans les figures suivantes correspondent aux REQA et REQB qui sont les premières requêtes du lecteur dans les normes ISO14443. Les figures II.10 et II.11 montrent l'importance du choix de l'antenne pour l'attaquant pour réaliser l'attaque la plus sensible. Pour ce test, le standard sans contact reste le même ; une distance d'espionnage de 4 mètres reste identique pour les deux tests. Le seul paramètre que l'on modifie est l'antenne de réception. Dans le premier cas, l'attaquant utilise une antenne standard, décrite dans la norme ISO 10373-6 (ISO). Dans le deuxième test, l'antenne utilisée est une antenne faite avec du câble coaxiale de 1 mètre de diamètre possédant un facteur de qualité très élevé (COAX). On observe que cette dernière antenne est bien plus sensible pour la réception de notre signal.

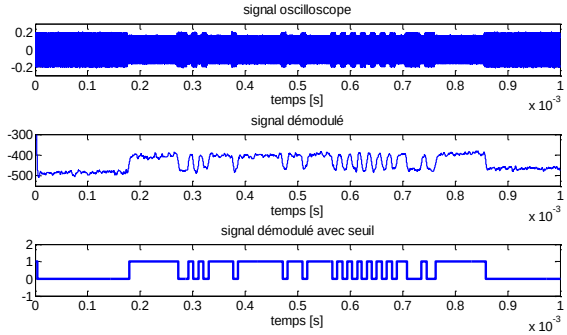


Figure II.10 – Signaux conformes au standard ISO14443-B enregistrés et démodulés sur l'antenne ISO pour d=4 m en position de Gauss 2

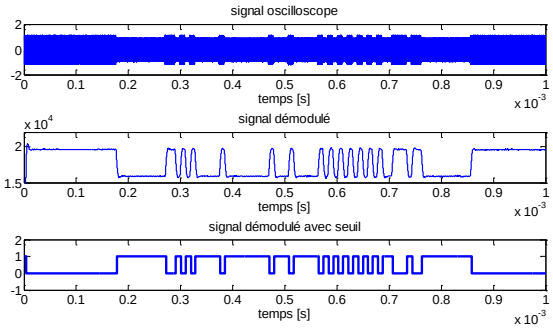


Figure II.11 – Signaux conformes au standard ISO14443-B enregistrés et démodulés sur l'antenne COAX pour d=4 m en position de Gauss 2

A 16 mètres, un attaquant est capable de réceptionner aussi bien le signal du lecteur pour les normes ISO14443-A que ISO14443-B. Cependant, on peut penser qu'il sera plus facile d'espionner les signaux conformes avec la norme ISO14443-A en raison de la modulation utilisée (modulation OOK). Les signaux ont été démodulés pour les deux positions de Gauss, on observe qu'à 16 mètres, c'est la position Gauss 1 qui permet de récupérer le mieux le signal (amplitude plus élevée). En théorie, c'est la position Gauss 2 qui devrait être la meilleure, mais le système de traitement et l'architecture du bâtiment peuvent influencer la réception des champs RF.

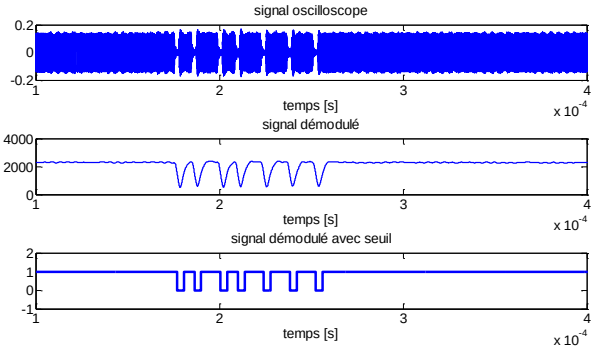


Figure II.12 – Signaux conformes au standard ISO14443-A enregistrés et démodulés sur l'antenne COAX pour d=16 m en position de Gauss 1

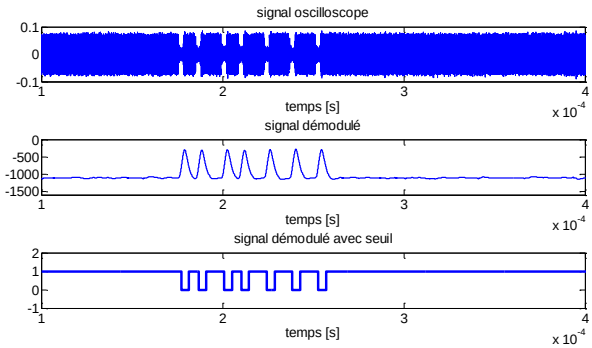


Figure II.13 – Signaux conformes au standard ISO14443-A enregistrés et démodulés sur l'antenne COAX pour d=16 m en position de Gauss 2

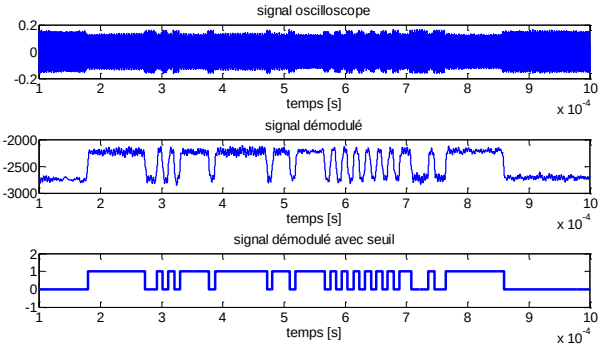


Figure II.14 – Signaux conformes au standard ISO14443-B enregistrés et démodulés sur l'antenne COAX pour d=16 m en position de Gauss 1

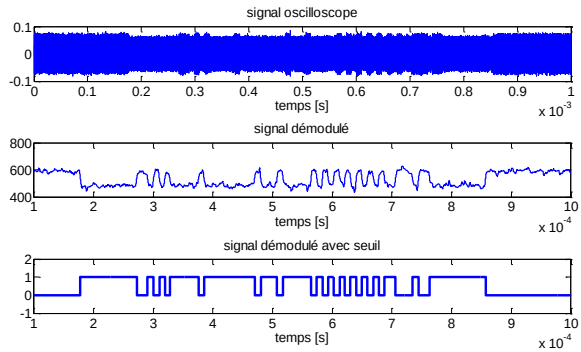


Figure II.15 – Signaux conformes au standard ISO14443-B enregistrés et démodulés sur l'antenne COAX pour d=16 m en position de Gauss 2

A 22 mètres, un attaquant peut encore réussir à détecter la requête du lecteur que ce soit en type A ou en type B (voir figure II.16 et II.17). Cette distance de 22 mètres correspond à plus de 220 fois la distance de fonctionnement d'un système sans contact. Après cette distance, le rapport signal sur bruit est trop faible et le système ne réceptionne plus les trames envoyées par le lecteur. On peut cependant se rendre compte du danger de ces attaques dans une gare pour récupérer les identifiants des cartes de transports, de la même façon près d'un terminal de paiement sans contact.

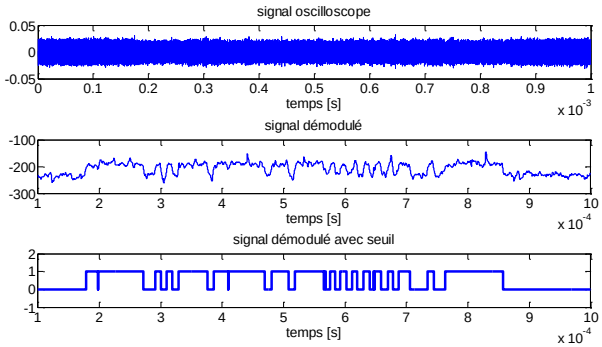


Figure II.16 – Signaux conformes au standard ISO14443-B enregistrés et démodulés sur l'antenne COAX pour d=22 m en position de Gauss 2

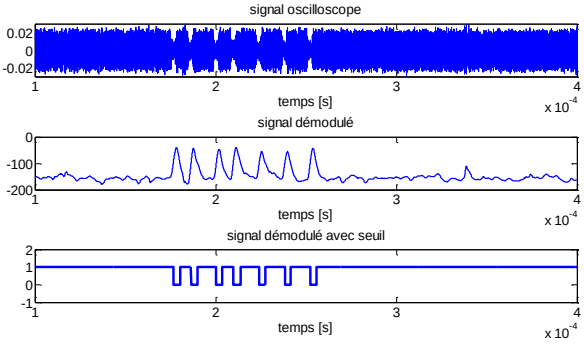


Figure II.17 – Signaux conformes au standard ISO14443-A enregistrés et démodulés sur l'antenne COAX pour d=22 m en position de Gauss 2

b. <u>Résultats de la voie de retour</u>

Les figures II.18 et II.19 correspondent aux signaux envoyés par la carte et enregistrés à deux distances différentes 1.5 m et 3.5 m. Pour chaque figure, on trouve le signal enregistré sur l'oscilloscope et le signal démodulé.

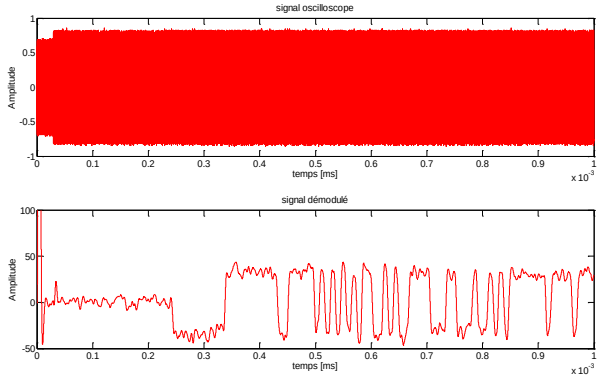


Figure II.18 – Signaux conformes au standard ISO14443-B enregistrés et démodulés sur l'antenne coaxiale pour d=1.5 m en position de Gauss 1

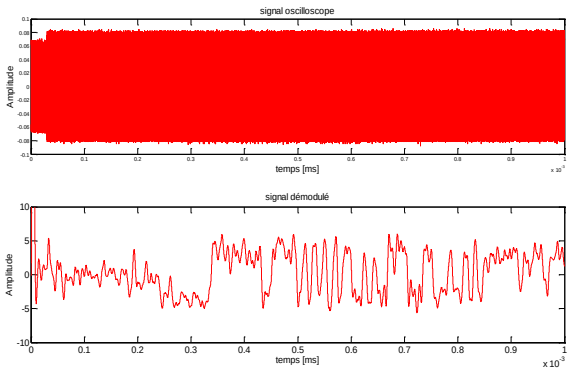


Figure II.19 – Signaux conformes au standard ISO14443-B enregistrés et démodulés sur l'antenne coaxiale pour d=3.5 m en position de Gauss 1

Il est possible d'espionner la communication de la carte vers le lecteur à une distance de 3.5 mètres de la source, ce qui correspond à 35 fois la distance nominale de communication entre le lecteur et la carte.

C. Cas particuliers

a. Antenne électrique

L'objectif de cette expérience est de montrer qu'il est possible d'espionner une communication entre un lecteur et une carte à quelques mètres avec un simple dipôle électrique (type antenne de voitures télécommandées).

Les tests effectués en extérieur donnent de bons résultats jusqu'à une distance de 4m ; la figure II.20 montre ces résultats. On observe un signal conforme à la norme ISO 14443-B envoyé par le lecteur.

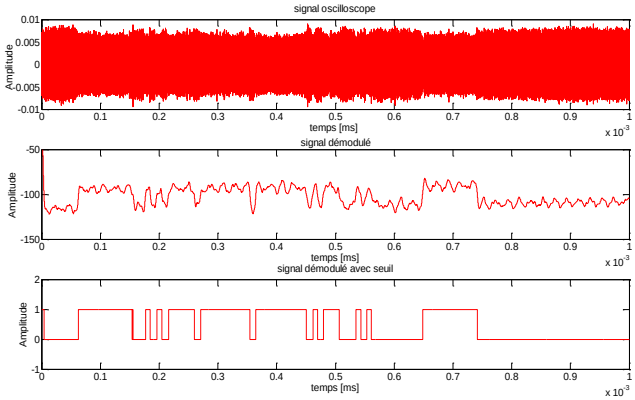


Figure II.20 – Signaux mesurés avec une antenne électrique à 4m de la source

b. Test sur une antenne trèfle

Des tests ont été réalisés avec la collaboration de Jérémy Chavat lors d'un stage de 2ème année d'école d'ingénieur pour étudier le champ à proximité d'une antenne dite trèfle. Ce type d'émetteur est constitué de plusieurs antennes et permet de générer un champ tournant. Une seule antenne de l'antenne trèfle est commandée par un lecteur Tagsys, l'antenne d'écoute est une simple antenne conforme à l'ISO10373. Une carte, voir la figure II.21, répertoriant les amplitudes maximales des signaux récupérés dans tout l'étage où est localisé l'antenne trèfle a été réalisée.

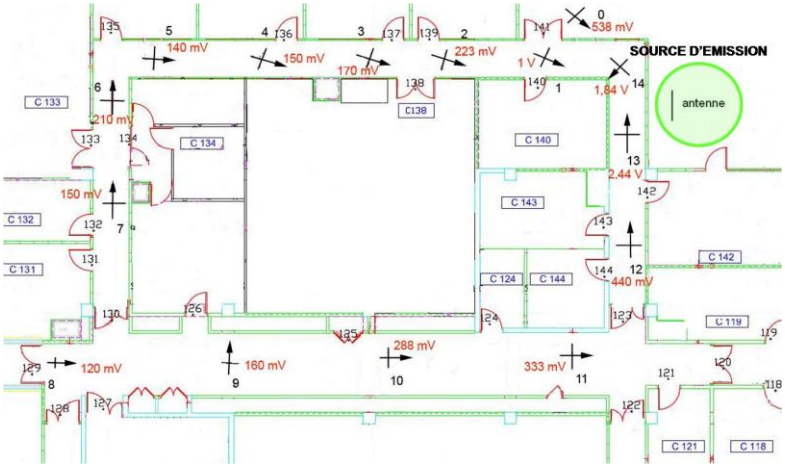


Figure II.21 – Ce plan du Rez-de-chaussée affiche les valeurs des maxima mesurées dans les couloirs aux alentours de l'antenne d'émission

On observe qu'il est possible d'espionner le signal du lecteur dans tout l'étage, avec des zones où le signal est plus fort alors que l'on est plus éloigné. L'amplitude du signal ne dépend donc pas que de la distance entre l'antenne espionne et l'antenne du lecteur, mais aussi d'autres paramètres.

Après des tests plus fins au niveau de ces zones, on peut penser que ces phénomènes sont dus aux conductions dans les câbles électriques et aux matériaux utilisés pour réaliser les cloisons, les structures métalliques par exemple.

c. Test sur une badgeuse

Au cours de nos premières expérimentations, nous avions remarqué la présence d'un signal à 13,56 MHz à la verticale d'une badgeuse située au 3ème étage dans le couloir central du BOC donnant accès à la pièce C412, voir la figure II.22. Jérémy Chavat a effectué des mesures d'eavesdropping plus ciblés. Ce signal très caractéristique est présent pendant 65 ms avec une récurrence de 85 ms.

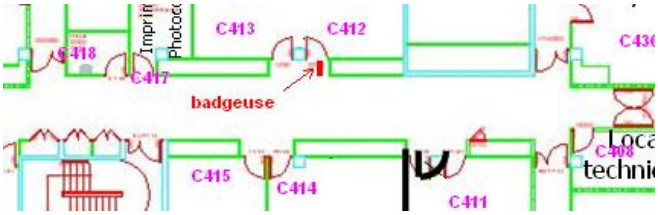


Figure II.22 – Plan du 3ème étage à proximité de la badgeuse

Des mesures ont été effectuées aux étages inférieurs à la verticale de la badgeuse. Le positionnement de l'antenne d'écoute doit être très précis. Elle doit être parallèle au mur et le plus près possible. Un décalage de quelques dizaines de centimètres vers la droite ou la gauche se traduit par la quasi-disparition du signal.

Les résultats montrent que le signal est encore bien visible deux étages en dessous de la badgeuse, mais que l'on a une perte du signal au rez-de-chaussée. La transmission des signaux se fait par la structure même des portes dont le cadre métallique fait office d'antenne et qui relaie le signal d'étage en étage.

4. Conclusion

Un système sans contact conforme aux normes ISO14443 type A ou type B comme celui que nous avons utilisé peut communiquer à une distance nominale d'une dizaine de centimètres. Nous avons observé au cours de ces tests qu'il est possible d'espionner une communication assez facilement entre un lecteur et une carte avec du matériel assez rudimentaire. La communication du lecteur vers la carte et de la carte vers le lecteur n'est pas espionnable à la même distance. Les tests réalisés ont montré qu'il est possible d'espionner une communication du lecteur vers la carte à plus de 20 mètres, mais que la communication de la carte vers le lecteur n'est visible qu'à moins de 3,5 mètres.

De plus, il a été montré que l'architecture du bâtiment peut jouer en faveur de l'attaquant, le réseau électrique et les cloisons à armatures métalliques transmettent très bien les signaux. La structure même du bâtiment crée de gros problèmes au niveau de la sécurité, l'environnement métallique est source potentielle de transmission de signaux.

PARTIE II. L'ATTAQUE RELAIS

L'attaque relais, voir la figure II.23, est une attaque qui permet à un attaquant d'établir une communication entre deux objets communicants qui ne sont pas dans la même zone de fonctionnement. Cette attaque, décrite par Conway en 1976, est basée sur le « Chess Grandmaster Problem ». Ce scénario montre comment une personne ne connaissant pas les règles du jeu d'échec peut cependant gagner au moins une partie en jouant contre deux champions d'échecs. Le principe est simple, il suffit d'opposer ces deux champions d'échecs dans

une même partie sans qu'il ne s'en rende compte en relayant leurs différents coups. L'attaque relais est simplement une transposition de ce problème au domaine de la sécurité.

La principale force de cette attaque est sa transparence vis-à-vis du système sans contact. En effet, il a été montré qu'un système sans contact classique était incapable de détecter une telle attaque bien que celle-ci implique une modification des temps de réponse de la carte. De plus, la cryptographie ne permet pas de compliquer l'attaque, car cette attaque implique la couche physique du système : le signal n'est pas décodé, il est transmis directement sans altération par le relais.

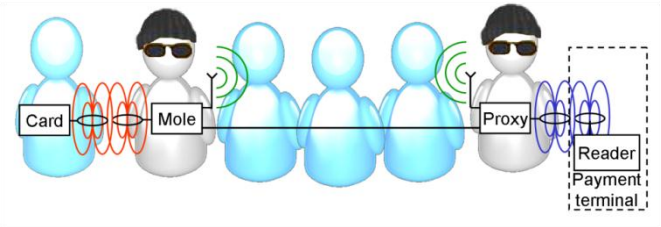


Figure II.23 – L'attaque relais

La cryptographie n'ayant aucun impact sur une telle attaque, le seul paramètre dépendant du relais qu'une contre-mesure peut mesurer ou calculer est le retard. Ce retard peut cependant être très faible et difficilement détectable. Cette partie a pour objectif la réalisation d'attaques relais introduisant des délais relativement faibles de façon à tester notre future contre-mesure.

1. Présentations de 3 nouvelles attaques relais

Actuellement, les principales implémentations d'attaques relais décrites dans la littérature ont été développées par G. Hancke ou T. Kasper. Ces auteurs utilisent des systèmes relais assez complexes en termes d'architectures électroniques, ce qui introduit un délai considérable dans le système sans contact existant. Ces relais, décrits dans la littérature, utilisent des composants tels que des microprocesseurs ou des puces permettant de démoduler ou de moduler un signal conforme aux standards du sans contact. Cette démodulation permet aussi de rendre le système relais compatible avec les standards de communications sans fil utilisées dans la liaison entre le môle et le proxy. Toutes ces étapes de traitement du signal ajoutent des délais importants dans le relais d'information.

Comme cela a été précisé dans la première partie, chaque norme utilisée par les systèmes sans contact précise des intervalles de temps entre la fin de l'émission de la requête lecteur et le début de la réponse carte (temps de retournement). Les relais développés par Hancke et Kasper sont conformes à la norme ISO14443-A dont la section 2 décrit le comportement au niveau de la couche physique, notamment ces temps de retournement. Malheureusement, ces contraintes temporelles sont difficiles à implémenter sur les systèmes actuels, car elles nécessitent une horloge de synchronisation très précise entre le lecteur et la carte. Ainsi, ces temps ne sont pas vraiment respectés par les développeurs de puces RFID, ce qui permet aux relais de type Hancke de pouvoir fonctionner. Notre objectif est de montrer qu'il est possible de réaliser des relais introduisant des retards imperceptibles par un lecteur sans contact qui serait conforme à la norme, mais aussi que la démodulation du signal n'est pas indispensable dans la réalisation d'un relais. Durant cette étude, deux types de relais ont été développés.

Le premier type de relais est dit filaire car le môle et proxy sont liés l'un à l'autre par un fil. Malgré le manque de transparence d'un tel système (un relais filaire est difficile à camoufler), un tel système a cependant tout son sens. En effet, de tels systèmes peuvent être utilisés dans une file d'attente par exemple ou dans des relais qu'on appellera figés (collet marseillais). De plus, la distance entre le lecteur et la carte peut quand même être importante (plusieurs mètres de câbles coaxiaux) et les délais introduit par de tels relais est très faibles.

Le deuxième type de relais est le relais sans fil ; ce relais se rapproche plus du relais dit Hancke. Cependant, comme cela sera vu ensuite, le délai introduit par ce type de relais est plus de dix fois inférieur à celui de Hancke.

De même que les communications sans contact utilisent un canal de transmission en full duplex (le médium air), les relais développés par la suite peuvent être assimilés à des canaux de communication full duplex puisque les signaux de la voie montante et de la voie descendante peuvent transiter en même temps. Pour faciliter la comparaison avec la littérature, les relais développés seront tous compatibles avec la norme ISO14443-A. L'objectif de cette étude est de développer les relais les plus rapides de façon à tester nos futures solutions.

A. Relais filaire

Le relais filaire est le plus simple système relais réalisé durant la thèse. Le design de ce relais en fait aussi un des plus simples qui puisse être réalisé par un attaquant potentiel. Cependant, ce relais est aussi le plus dangereux puisque, comme nous le démontrerons plus tard, il peut introduire des délais très faibles, proches de la porteuse du signal émis, soit 1/13.56e6=73.74ns. Cette attaque, décrite par la figure II.24, déporte simplement le signal du lecteur sur une distance L correspondant à la longueur du câble coaxial. Le signal déporté n'est absolument pas modifié, on ne touche pas aux données transmises par le lecteur ou par la carte, notre relais ressemble à une version filaire d'un système sans contact. Le problème d'un tel système est qu'il peut être complètement légitime, dans le sens où il peut permettre de transmettre des signaux RF entre un lecteur et une carte situés dans deux zones différentes, ces deux zones étant séparées par un mur par exemple. Par ailleurs, le brevet FR2896898 décrit le fonctionnement d'un système similaire permettant de déporter un signal sur quelques mètres [CHA2007].

La réalisation d'une telle attaque est très simple, le matériel nécessaire consiste en un simple câble coaxial de la longueur voulue et de deux antennes adaptées à l'impédance caractéristique du câble (en général 50Ω) et accordées à 13.56 MHz, la fréquence de notre système sans contact.

Une conception aussi simple permet au relais d'induire des délais très faibles, ce qui est une grande menace pour la sécurité des systèmes sans contact. Ce retard est principalement dû au temps de propagation du signal dans l'air et dans le câble coaxial, soit quelques dizaines de nanosecondes ainsi que le temps d'établissement de ce même signal dans les antennes, un temps un peu plus important qui dépend des caractéristiques physiques des antennes.

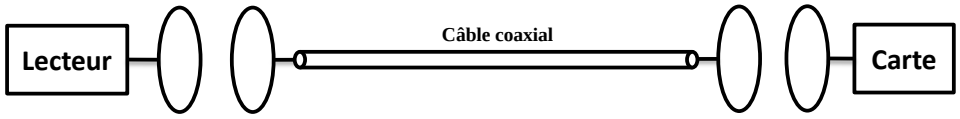


Figure II.24 – Relais passif filaire

Les seuls circuits réalisés pour ce relais sont les deux antennes, et les circuits d'adaptation. Plus d'explications sur la fabrication des antennes sont données en annexe.

La figure II.25 présente le relais filaire réalisé tandis que la figure II.26 présente une possibilité d'utilisation d'un tel relais.

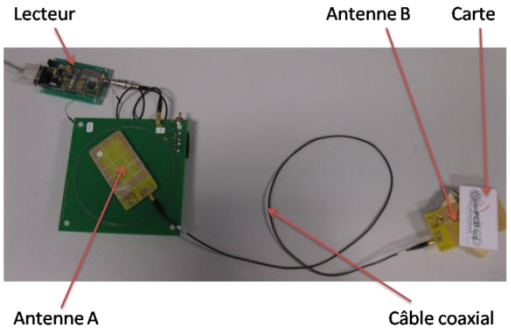


Figure II.25 – Photo d'un relais filaire

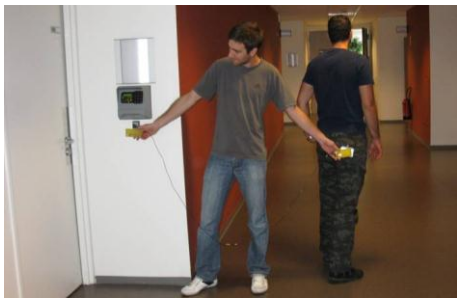


Figure II.26 – Utilisation d'un relais filaire

Un relais similaire a été développé par Capkun et Francillon en 2010 sur des systèmes sans contact à 125 kHz utilisés dans les clés de voitures actuelles [FRA2011]. En plus de la gamme de fréquences qui n'est pas la même, les données dans le relais développé ne circulent que dans un sens (canal de communication simplex).

B. Relais avec démodulation de la voie retour

L'objectif de ce second relais, voir la figure II.27, est de recréer la modulation de charge de la carte à proximité de l'antenne du lecteur de façon à rendre la détection du relais plus difficile. En effet, le front-end du proxy dans ce design est similaire à celui d'une carte sans contact. Contrairement au relais filaire, il n'y a pas réinjection de champ RF au niveau de l'antenne du proxy. Le lecteur n'a ici aucun moyen d'identifier le relais en observant son champ RF, ce qui pourrait être le cas avec le relais filaire.

La voie montante de ce relais est très proche de l'étage de sortie d'un lecteur utilisé pour faire du skimming (activation à distance de carte), on amplifie simplement le signal récupéré sur l'antenne A-1 (voie 1 de l'antenne marguerite proche du lecteur). La voie de retour est plus complexe. Pour recréer la modulation de charge à proximité du lecteur, il est nécessaire de démoduler dans un premier temps le signal envoyé par la carte. Dans un second temps, un transistor commute la charge qui permettra de moduler le champ du lecteur. Le signal est donc démodulé en utilisant un démodulateur synchrone. Le signal de la carte permet de définir une horloge de synchronisation, permettant de démoduler le signal de la carte par transposition de fréquence. Le signal doit ensuite être remis en forme pour obtenir un signal binaire modulé à la fréquence de la sous-porteuse de notre signal HF. Ce signal permet de moduler la charge connectée à l'antenne B-2.

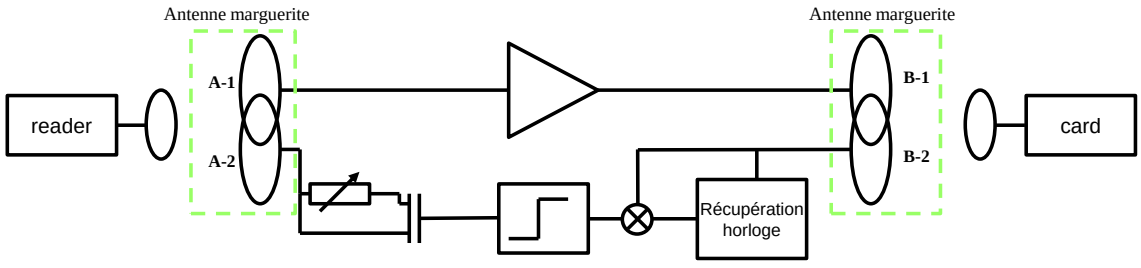


Figure II.27 – Topologie d'un système relais filaire avec démodulation

Les antennes A et B sont des antennes dites marguerites, elles combinent chacune deux antennes présentant une mutuelle nulle entre elles. Ces antennes ont été développées dans le cadre d'un DRT (Diplôme de Recherche Technologique) au CEA et ont fait l'objet d'un brevet FR2923324 [SAB2007]. L'objectif est d'éviter que ces deux antennes se perturbent entre elles. Cette particularité est très utile dans ce type de relais pour éviter que le signal du lecteur et le

signal du proxy ne s'ajoutent. De plus, un avantage de ces antennes est qu'elles ont toutes les deux le même diagramme de rayonnement.

La figure II.28 présente le relais avec démodulation réalisé.

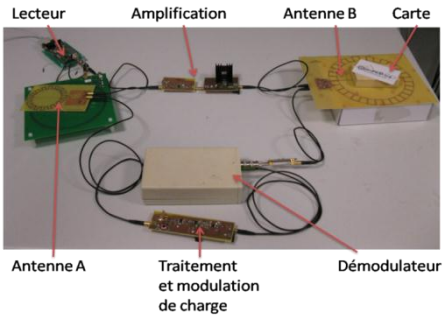


Figure II.28 – Photo d'un relais filaire avec démodulation

C. Relais wireless

Ce relais est le seul relais sans fil présenté dans cette section réservée aux relais rapides. Nous rappelons que l'objectif est avant tout de réaliser des relais qui introduisent des délais très faibles. Ce relais est donc assez similaire à celui mis au point par Hancke dans le sens où il n'est théoriquement pas limité spatialement par le lien filaire. La figure II.29 décrit une architecture simplifiée de ce type de circuit. Le lien sans fil est plus complexe que celui utilisé par G. Hancke car nous ne démodulons pas le signal de façon à obtenir un relais très rapide, le signal est simplement surmodulé à une fréquence supérieure à la fréquence HF du signal lecteur (ce système est dit superhétérodyne).

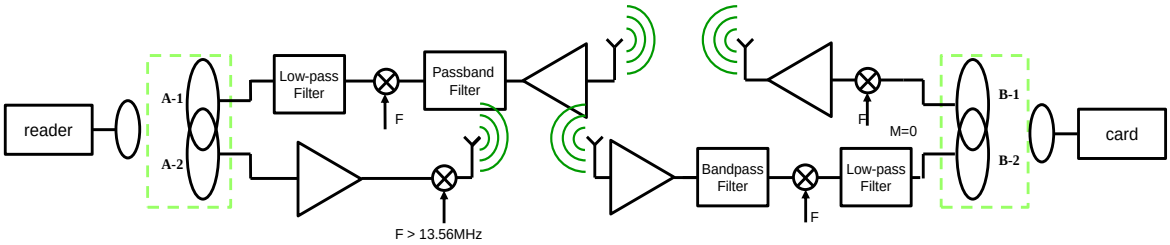


Figure II.29 – Topologie d'un relais superhétérodyne

Comme pour le précédent relais, les antennes A et B sont des antennes marguerites présentant une mutuelle nulle entre leurs deux antennes. Le signal lecteur est reçu sur l'antenne A-1 et mélangé avec une fréquence plus élevée (900 MHz dans notre cas) que la fréquence HF du signal. Le signal de fréquence fixe F de 900 MHz mélangé avec le signal utile est généré par une PLL (boucle à verrouillage de phase). Le signal sur-modulé doit encore être amplifié avant d'être émis par l'antenne de type dipôle. Le signal radiofréquence est reçu sur une deuxième antenne électrique, le signal doit être amplifié et filtré avant d'être démodulé à l'aide d'un nouveau mélangeur dont la valeur de la fréquence LO sera F. Le signal doit alors être filtré pour récupérer notre signal utile, le signal issu du lecteur et l'envoyer vers la carte par l'antenne B-1. La voie descendante du montage est presque identique à la voie montante, on transmet le champ RF au niveau de l'antenne B-2 en le modulant afin de le récupérer finalement au niveau de l'antenne A-1 après démodulation. Le principe de ce système est expliqué par la figure II.30.

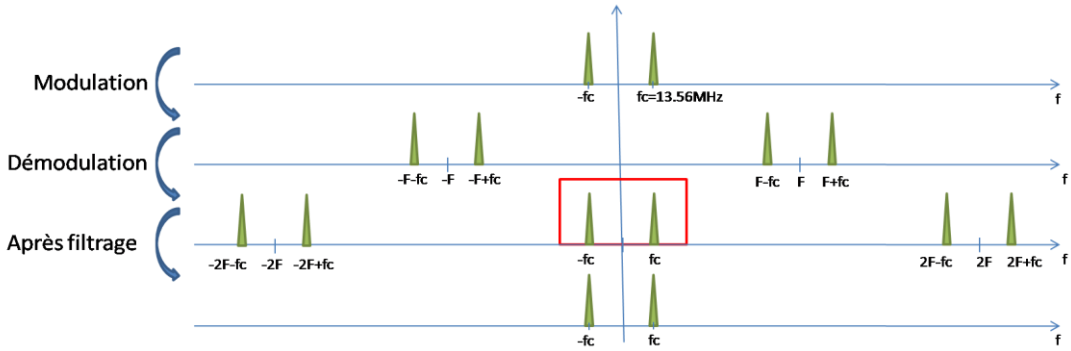


Figure II.30 – Modulation et démodulation du signal

Ce relais peut être associé avec celui avec démodulation pour recréer la modulation de charge à proximité du lecteur. Ce relais a été particulièrement difficile à réaliser bien que le principe de base soit pourtant simple. Pour obtenir un signal démodulé cohérent, le rapport signal sur bruit doit rester élevé. De même, les deux PLLs (proxy et môle) doivent générer exactement la même fréquence de façon à ne pas créer un glissement de fréquence et l'introduction d'une fréquence basse. Le système complet n'a jamais été réalisé de façon complète, car le besoin en matériel électronique était trop important. Selon les tests à réaliser, le circuit a été adapté pour simplifier notre travail. La figure II.31 présente uniquement la voie montante du relais superhétérodyne.

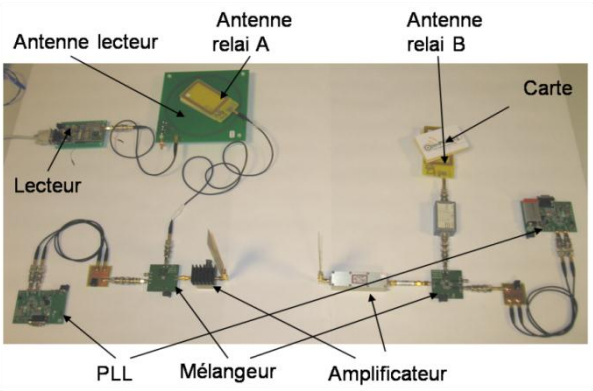


Figure II.31 – Photo du relais superhétérodyne (voie montante)

2. Relais filaire et augmentation de la puissance de l'antenne d'émission

Lors d'expériences réalisées sur les relais filaires, nous avons remarqué que le champ émis par le lecteur était plus grand en présence d'un relais qu'en présence d'une simple carte. Lors d'une expérience en particulier, nous avons par ailleurs «grillé» un lecteur sans contact mis en présence d'un relais filaire. Nous avons cherché à déterminer la cause de cette augmentation de la valeur de champ RF en travaillant sur les équations de transfert du système relais filaire.

Le lecteur utilisé dans un système sans contact peut être modélisé par un circuit R, L, C en série (Ra, C1, L1). Ce circuit d'antenne est alimenté par un générateur de tension sinusoïdale de fréquence 13.56 MHz et de résistance interne R_0. De la même façon, une carte sans contact peut être modélisée par un circuit R, L, C en parallèle. Les deux circuits interagissent ensemble par le biais de la mutuelle M_{14}. L'ensemble est décrit par la figure II.32.

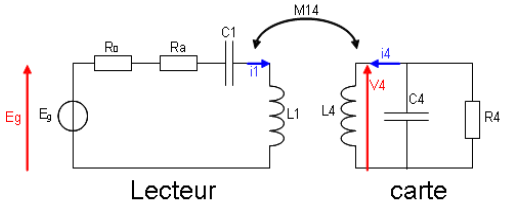


Figure II.32 – Système sans contact

Le relais est simplement constitué de deux antennes modélisées par des systèmes R, L, C en parallèle et un câble coaxial. En négligeant l'atténuation et l'effet du câble coaxial du relais (simplification des équations), le relais filaire peut être assimilé à deux circuits antennes. Il existe une mutuelle M_{12} entre l'antenne lecteur et la première antenne du relais. De la même façon, il existe une mutuelle M_{34} entre l'antenne de la carte et la deuxième antenne du relais. Le schéma électrique équivalent du système sans contact lié par un relais de type filaire est illustré à la figure II.33.

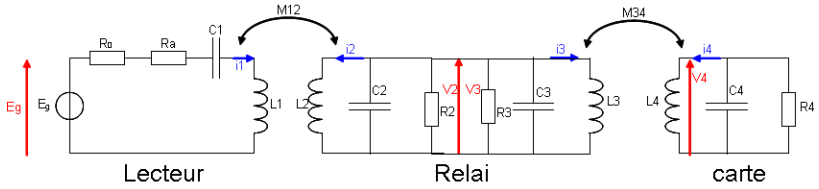


Figure II.33 – Système sans contact avec relais filaire

Les fonctions de transfert de ces deux systèmes sont déterminées par le rapport entre le courant dans l'antenne du lecteur sur la tension du signal d'entrée Eg. Plus d'informations sur les équations des systèmes et sur leurs fonctions de transfert globales sont données en annexe. Les fonctions de transfert sont ensuite simulées sous Simulink ; on trace les réponses impulsionnelles de ces deux systèmes, voir la figure II.34.

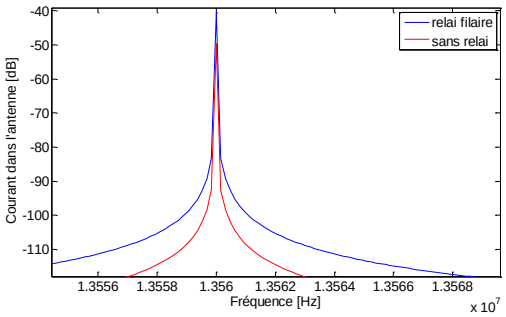


Figure II.34 – Courant dans l'antenne du lecteur dans le cas avec et sans relais

Par la simulation, on trouve un gain en amplitude de 3 entre le cas avec et sans relais. Cette valeur est conforme avec la valeur mesurée lors d'expérimentations puisque les bobines de calibration indiquaient une variation de 3 à 9 A/m lors de la mise en place du relais. Les cas critiques d'amplification n'ont pas été étudiés puisque l'on a choisi certaines valeurs de composants. Cependant, il est possible de dire que pour certains couplages entre les antennes, la mise en place d'un relais dans le système augmente de façon importante l'amplitude du champ radiofréquence du lecteur. Cette forte augmentation du courant dans l'antenne du lecteur peut détruire le lecteur ou la carte sans contact.

3. Expériences réalisées sur les relais

Deux types d'expériences ont été réalisés : la première a permis de prouver le fonctionnement des relais et de déterminer certaines caractéristiques comme la distance d'activation ou l'atténuation du signal ; la deuxième expérience a pour objectif la mesure des délais introduits par les différents relais.

Le banc de test utilisé, voir la figure II.35, est approximativement le même pour les deux expériences, le lecteur est connecté à l'ordinateur, la carte est placée à quelques mètres du lecteur. L'un des trois relais est placé entre le lecteur et la carte.

L'oscilloscope utilisé pour enregistrer le signal est un 735Zi Lecroy Wavepro, de bande passante 1,5 GHz et de fréquence d'échantillonnage de 40GS/s. Les sondes de champ, utilisées pour visualiser et enregistrer le signal sur l'oscilloscope sont au format ID1 et ont une sensibilité de 6A/m/V. La première sonde de champ est placée contre l'antenne du lecteur et la seconde contre la carte sans contact. L'antenne A du relais est celle placée côté lecteur et l'antenne B du relais près de la carte.

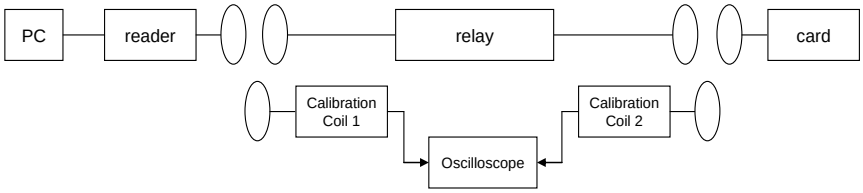


Figure II.35 – Banc de test

A. Première série d'expériences

Pour cette série de tests, le système sans contact utilisé est conforme à la norme ISO14443-A : l'objectif principal est de prouver que nos relais transmettent les données entre un lecteur et une carte du commerce. Le lecteur utilisé pour cette expérience est un lecteur de la société Inside Contactless compatible avec la norme ISO 14443-A. Ce lecteur est connecté à une antenne conforme à la norme ISO qui a un facteur de qualité de 10. La carte sans contact utilisée est une carte Mifare Classic 1k. La longueur des relais est de 2 mètres de câble coaxial mais cette longueur ne fait pas vraiment varier les caractéristiques du système relais. La figure II.36 présente le système de mesure de cette première expérience.

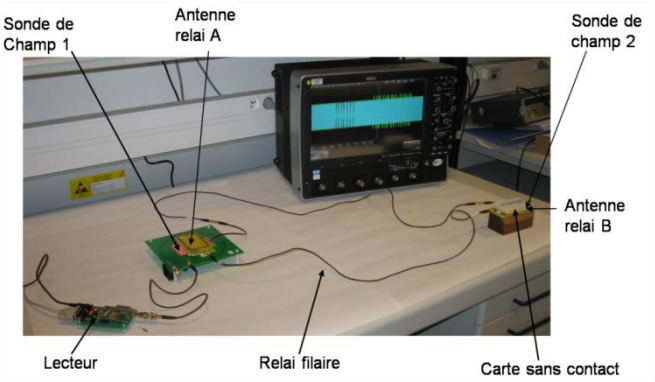


Figure II.36 – Banc de test pour la première série d'expériences

a. Mesure d'atténuation et conformité avec la norme

L'atténuation du signal dans le relais est une information importante, car elle montre l'effet du relais sur le signal. Cette information dépend fortement de la conception du relais ; les paramètres qui ont un effet sur l'atténuation sont la longueur du câble, le couplage entre les antennes et le traitement du signal (amplification, démodulation,…). Pour mesurer l'atténuation de la voie

montante, on s'intéresse à l'amplitude du champ RF côté carte et côté lecteur. Pour la voie descendante, il est intéressant de vérifier la concordance avec la norme ISO14443-A en calculant l'amplitude de la sous-porteuse avec un banc de test conforme à la norme ISO10373, voir la figure II.37.

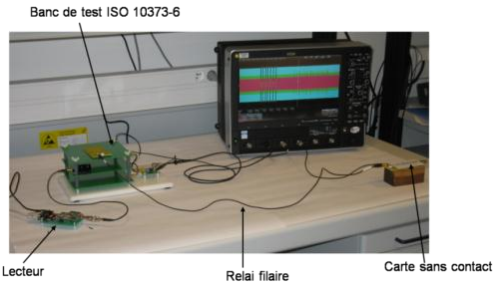


Figure II.37 – Mesure de l'amplitude de la modulation de charge

Ces informations sont données pour un système sans contact simple. La distance entre les différentes antennes du relais et du système sans contact ne sont pas nulles ; nous utilisons 1 cm pour réduire le couplage entre les antennes.

Pour un système sans contact, l'affaiblissement du signal de la voie montante à 1 cm est de -1,53 dB et la norme ISO impose une amplitude de modulation de charge d'au moins $30/H^{1.2}$ (mV crête) où H est la valeur efficace du champ magnétique en A/m. Dans notre test, la valeur de H est de 2 A/m ce qui implique que la modulation de charge doit être supérieure à 13 mV RMS pour être en conformité avec la norme.

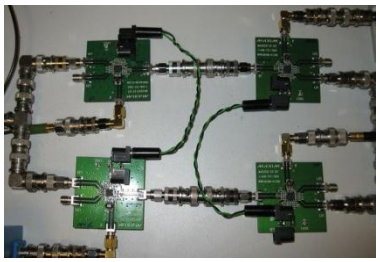


Figure II.38 – Circuit superhétérodyne sans antennes

Dans le cas du relais sans fil, l'amplitude de la modulation de charge a été mesurée sans les antennes électriques, car sa voie descendante était trop difficile à mettre en place. Le signal est donc uniquement modulé et démodulé avec l'utilisation des mixers (figure II.38).

Le tableau II.1 donne les valeurs trouvées pour l'atténuation et l'amplitude de la modulation de charge pour les différents relais.

Tableau II.1 – Caractéristiques des relais

	Relais filaire	Relais filaire avec démodulation	Relais sans fil
Atténuation (voie montante)	-4.3dB	-5.4 dB	-6.1 dB
Amplitude de la modulation de charge	14.17 mVp	14 mVp	14 mVp

Ces données sont difficiles à interpréter dans le sens où l'insertion d'un relais sans démodulation implique l'apparition de nouveaux champs électromagnétiques. Le relais filaire, comme on l'a vu auparavant, augmente la valeur du champ RF à proximité du relais. On peut cependant dire que le signal carte au niveau du lecteur est en conformité avec la norme puisque

l'amplitude de la modulation de charge pour les différents relais est au-dessus de la norme fixée par les normes sans contact.

b. Distance d'activation

Il est possible de faire varier différents facteurs tels que la longueur du relais, la distance entre le lecteur et le proxy ou la distance entre la carte et le môle. Faire varier la distance lecteur-proxy n'est pas vraiment intéressant parce que l'attaquant peut placer le proxy sur l'antenne du lecteur. À l'inverse, la distance mole-carte est une indication importante sur le rendement du relais car l'attaquant ne peut pas contrôler cette distance. Plus cette distance est importante et plus l'attaquant pourra s'éloigner de sa victime. Il est donc important de mettre l'accent sur la distance d'activation maximale de la carte pour chaque attaque relais. Pour un système sans contact sans relais, la distance d'activation est proche de 10 cm. Dans le cas du relais sans fil et pour connaître la distance d'activation de la carte, nous avons utilisé le Proxispy (analyseur de protocoles sans contact) pour ne pas implémenter la voie descendante. Le tableau II.2 résume les valeurs de distance d'activation trouvées pour les différents relais.

Tableau II.2 – Distance d'activation

	Relais filaire	Relais filaire avec démodulation	Relais sans fil
Distance d'activation	6 cm	8 cm	8 cm

Ces résultats sont uniquement vrais pour une certaine configuration de l'attaque, on obtiendra des résultats différents pour une topologie différente : facteur de qualité des antennes, longueur physique du relais, amplification différente, ….

c. Coût et complexité

Le coût et la complexité sont importants pour déterminer les ressources nécessaires à un attaquant pour une telle attaque relais, voir tableau II.3.

Tableau II.3 – Complexité et cout des relais

	Relais filaire	Relais filaire avec démodulation	Relais sans fil
Coût	*	**	*****
Complexité	*	***	****

B. Deuxième série d'expériences : Mesure de délais

L'objectif principal de cette seconde expérience est de mesurer les retards introduits par les trois relais. Les retards introduits par certains de ces relais sont si faibles qu'il n'est pas possible de les voir à l'œil nu, voir la figure II.39. Il est aussi difficile de mesurer ces retards avec un système sans contact classique.

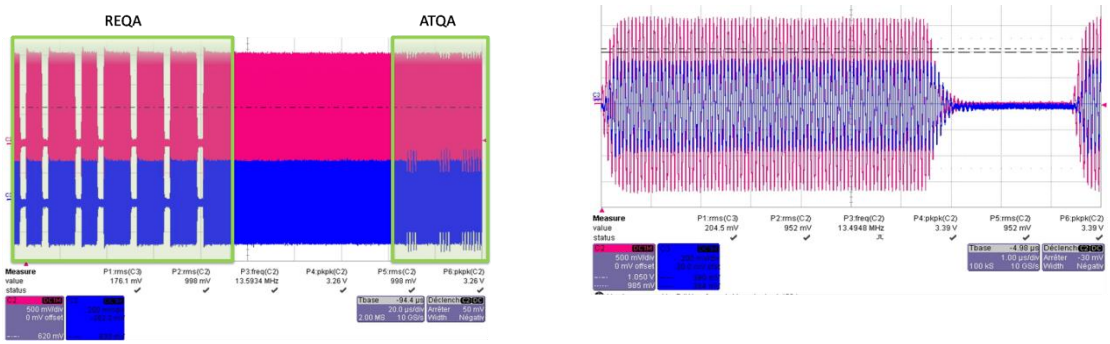


Figure II.39 – Courbes obtenues pour le relais filaire (magenta = signal lecteur, bleu: signal carte)

Pour mesurer de tels délais, il est possible de calculer la corrélation entre deux séquences enregistrées à l'aide d'antennes de chaque côté du relais. Il est alors nécessaire d'utiliser des signaux ayant des propriétés de corrélation intéressantes. En utilisant un lecteur «Ouvert» développé au sein du CEA Léti (Lrfv7-2), il est possible d'envoyer le signal désiré, voir la figure II.40. Les propriétés de ces signaux et la façon de les corréler sont étudiées dans le prochain chapitre. Ce signal est modulé en amplitude et possède une sous-porteuse à 848 kHz.

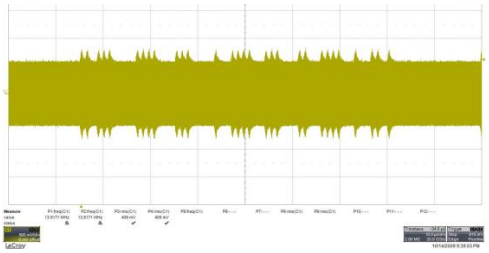


Figure II.40 – Signal envoyé par le lecteur Lrfv7-2

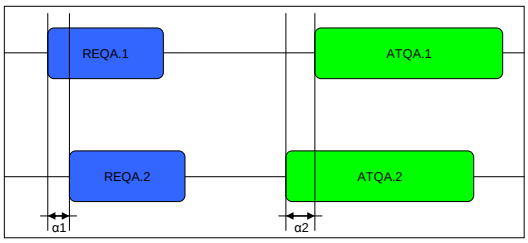


Figure II.41 – Retard de propagation

Si l'on place un relais entre le lecteur et la carte sans contact, il existe un retard α_1 entre l'émission du REQA par le lecteur et celui reçu par la carte et un retard α_2 pour l'ATQA envoyé par une carte et celui reçu par le lecteur (figure II.42). La voie montante et la voie descendante du relais étant différentes, les retards α_1 et α_2 peuvent être différents selon le relais utilisé.

Les délais ont donc été mesurés pour chaque partie du relais (voie montante et voie descendante) et sommés pour obtenir le délai total induit par un relais. Cette expérience est reproduite pour différents couplages entre l'antenne du lecteur et l'antenne du relais. En effet, ce couplage a une incidence sur le temps d'établissement du signal dans les antennes. Après l'échantillonnage de 1 GS/s, les signaux enregistrés sont corrélés sur Matlab ; l'index correspondant au maximum de corrélation représente le délai entre les deux signaux.

Pour comparer les retards, il est nécessaire de mesurer aussi le retard pour une transmission du signal entre le lecteur et la «carte» hors présence d'un relais.

Le tableau II.4 présente les résultats de délais dans les cas avec et sans relais.

Tableau II.4 – Délais mesurés

Distance antenne lecteur – antenne A relais	Relais filaire	Relais filaire avec démodulation	Relais sans fil	Sans relais
1 cm	295 ns	1.5µs	566ns	-66ns
3 cm	442 ns	1.66µs	454ns	-44ns
8 cm	442 ns	1.7µs	652ns	-22ns

Les pics de modulation, voir la figure II.43, donnent une première estimation du retard entre les deux signaux. Le résultat est surprenant : les pics rouges (correspondant au signal carte) arrivent avant les pics bleus (correspondant au signal lecteur). Un zoom sur un pic de modulation permet de comprendre cet effet visuel, le début du pic de modulation bleu est bien avant le début du pic de modulation rouge, mais l'amplitude des pics de modulation donne l'impression que le maximum du pic rouge arrive avant le maximum de le pic bleu.

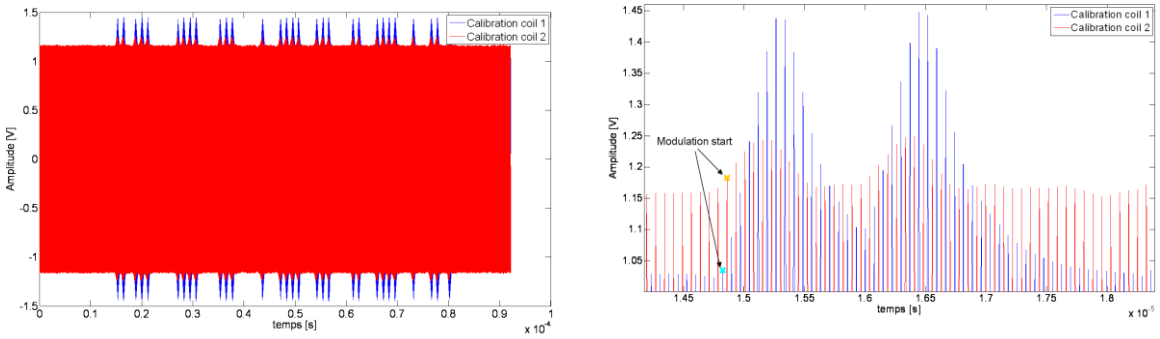


Figure II.42 – Signal à corréler (rouge = signal carte, bleu: signal lecteur)

Les résultats obtenus dans le cas sans relais sont négatifs et varient entre -22 et -66 ns. Un retard négatif implique que le signal enregistré sur la sonde de champ 2 arrive avant le signal enregistré sur la sonde de champ 1, ce qui est impossible puisque le signal est envoyé par le lecteur. Ces résultats confirment cependant les formes de signaux observés sur l'oscilloscope.

Ces retards négatifs démontrent que le calcul de corrélation est sensible à l'amplitude des pics de modulation. Nous reviendrons sur ce point dans la partie suivante.

Le retard obtenu avec un relais dépend de trois caractéristiques du relais : le temps d'établissement dans les antennes, le temps de propagation dans le câble et le traitement des signaux par le relais.

En conclusion, pour deux signaux dont la modulation de charge est d'amplitude égale, le retard augmente avec la distance entre les antennes. Cependant, si les deux signaux ont des amplitudes de modulation de charge différentes, le retard peut diminuer même si la distance augmente.

La figure II.42 donne une vue globale des délais calculés pendant la deuxième expérience. Chaque relais est caractérisé par un intervalle de temps, il est possible de différencier les différentes formes de relais. Les retards calculés dans le cas avec démodulation sont plus importants que les autres car le traitement des signaux prend du temps. Le relais sans fil et le relais filaire ont des retards proches car le mélange des signaux est très rapide.

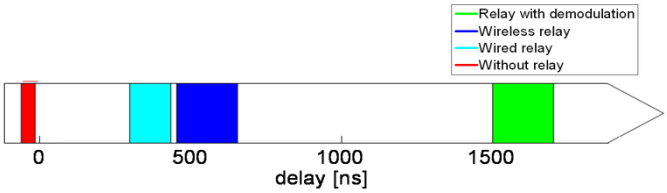


Figure II.43 – Vue globale des délais induits par le relais

C. Précision des délais mesurés

L'objectif de cette partie est de déterminer la précision de nos mesures de délais.

a. Précision d'un signal modulé avec porteuse fc

Il y a un pic de corrélation lorsque les deux signaux sont en phase ou en opposition de phase. En théorie, le délai obtenu par corrélation est égal à 1/(2*fc) avec fc la fréquence de la porteuse de notre signal, soit 36,87 ns. Le signal étant échantillonné à 1 GS/s, nous pouvons détecter une différence de phase de 1 ns entre les deux signaux, la corrélation a donc théoriquement une précision comprise entre 36 et 37 ns.

b. Influence des temps d'établissement du signal sur la précision

Le résultat précédent est correct lorsque les signaux corrélés sont identiques, mais le temps d'établissement des signaux peut modifier le résultat de cette corrélation. Soit un signal x, illustré à la figure II.44-A, envoyé dans un canal de communication tel que y, illustré à la figure II.44-B, soit le signal après traitement par une fonction de transfert h. Le signal y reçu n'a pas les mêmes temps d'établissement que le signal envoyé x.

La corrélation entre un signal x et un signal y est donnée par l'équation II.4 :

$$Rxy(k) = \sum_{n=-\infty}^{\infty} x(n+k).y(n) = \sum_{n=-\infty}^{\infty} x(n).y(n+k) \qquad \text{(II.4)}$$

Nous avons calculé la valeur de corrélation pour les trois valeurs de retard correspondantes aux figures II.44-C, II.44-D et II.44-E

$$Rxy(0) = \sum_{n=1}^{16} x(n).y(n) = 105 \qquad \text{(II.5)}$$

$$Rxy(1) = \sum_{n=1}^{16} x(n+1).y(n) = 98 \qquad \text{(II.6)}$$

$$Rxy(-1) = \sum_{n=1}^{16} x(n-1).y(n) = 106 \qquad \text{(II.7)}$$

Le premier cas, voir équation II.5, illustré à la figure II.44-D, correspond à la corrélation calculée pour un retard nul. Si l'on se base sur la théorie, la valeur de corrélation trouvée devrait être maximale pour cette valeur de délai.

Le deuxième cas, voir équation II.6, illustré à la figure II.44-C, est la valeur de corrélation calculée lorsque l'on avance le signal x d'un échantillon. Nous trouvons une valeur de 98, cette valeur est donc inférieure à celle trouvée pour un retard nul.

Le troisième cas, voir équation II.7, illustré à la figure II.44-E, est la valeur de corrélation lorsque notre signal x recule d'un échantillon. Nous trouvons une valeur de 106 plus élevée que pour un retard nul. Nous montrons par cet exemple que la valeur de corrélation d'un signal est liée à la symétrie des pics de la modulation de sous-porteuse.

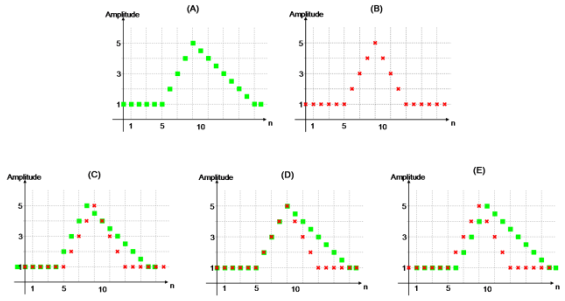


Figure II.44 – Précision vs temps d'établissement

c. Influence de l'amplitude de la sous-porteuse du signal sur la précision

On montre ici que la précision de nos mesures dépend fortement de l'amplitude de notre sous-porteuse et que l'on peut trouver des résultats très différents si les amplitudes des deux signaux à corréler sont différentes. Les signaux des figures II.45-A et II.45-B correspondent à deux signaux possédant une amplitude différente.

La valeur de corrélation est calculée pour les trois valeurs de retard correspondantes aux figures II.45-C, II.45-D et II.45-E

$$Rxy(0) = \sum_{n=1}^{16} x(n).y(n) = 65 \quad \text{(II.8)}$$

$$Rxy(1) = \sum_{n=1}^{16} x(n+1).y(n) = 67 \quad \text{(II.9)}$$

$$Rxy(2) = \sum_{n=1}^{16} x(n+2).y(n) = 65 \quad \text{(II.10)}$$

Le premier cas, voir équation II.8, illustré à la figure II.45-D, correspond à la corrélation calculée pour un retard nul. Si l'on se base sur la théorie, la valeur de corrélation trouvée devrait être maximale pour cette valeur de délai.

Le deuxième cas, voir équation II.9, illustré à la figure II.45-C, est la valeur de corrélation calculée lorsque l'on avance le signal x de deux échantillons. Nous trouvons une valeur de 65, cette valeur est donc égale à celle trouvée pour un retard nul.

Le troisième cas, voir équation II.10, illustré à la figure II.45-E, est la valeur de corrélation lorsque l'on avance le signal x d'un échantillon. Nous trouvons une valeur de 67 plus élevée que pour un retard nul. Nous montrons par cet exemple que la valeur de corrélation d'un signal est liée à la symétrie des pics de la modulation de sous-porteuse.

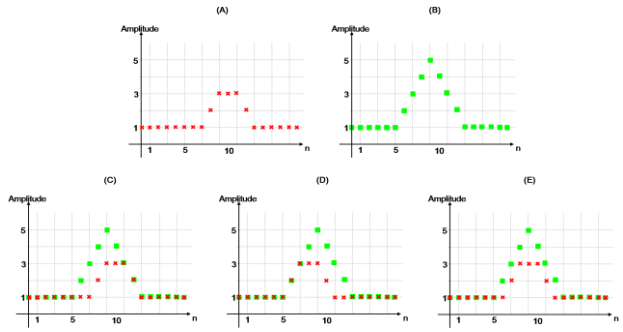


Figure II.45 – Précision vs amplitude la sous-porteuse

d. Conclusion

Tout ceci explique pourquoi la résolution de corrélation est moins précise que 1 / (2 * fc). Le temps d'établissement et l'amplitude de la sous-porteuse peuvent ajouter une erreur non négligeable à la période de la porteuse.

4. Relais avec traitement du signal

Après avoir travaillé sur les relais dits «rapides» (c'est-à-dire introduisant un délai très faible durant la transmission du signal), nous avons jugé intéressant de réaliser un relais plus évolué. Ce relais est très proche de ceux développés par Hancke et Kasper ; le signal est décodé de façon à posséder une compatibilité avec n'importe quel système de transmission sans fil entre le proxy et le môle (figure II.46). Cependant, nous avons toujours à cœur de réaliser un système plus rapide. Réaliser un relais dont le signal est entièrement démodulé est plus complexe pour un attaquant, car il doit avoir une parfaite connaissance de la norme sans contact utilisée par les systèmes qu'il souhaite pirater. Sans avoir besoin d'acheter la norme correspondante, on trouve toutes les informations nécessaires sur internet concernant la modulation et la démodulation des signaux

codés. Nous avons choisi de développer un système compatible avec la norme ISO14443-A de façon à comparer plus facilement notre système avec la littérature. Cependant, le système est rapidement adaptable à une autre norme sans contact comme l'ISO14443-B ou l'ISO15693.

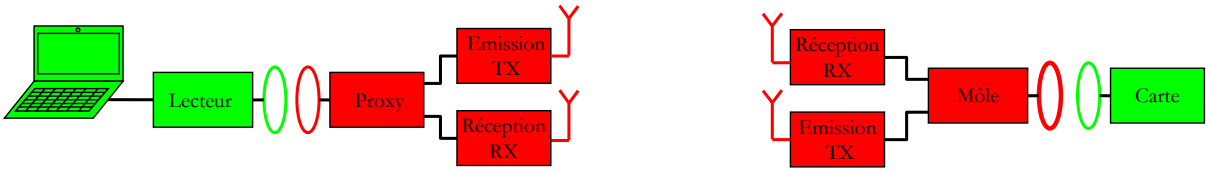


Figure II.46 – Système complet

A. Le proxy

Pour réaliser la carte électronique du proxy, nous n'avons pas voulu recréer l'existant et nous nous sommes basés sur la carte développée par Timo Kasper durant sa thèse [CAR2006]. Cette carte électronique peut être divisée en deux sous-systèmes : l'un permettant la démodulation et la mise en forme du signal lecteur et l'autre recréant la modulation de charge au niveau du lecteur. Ces deux sous-systèmes sont détaillés par la suite, voir la figure II.47.

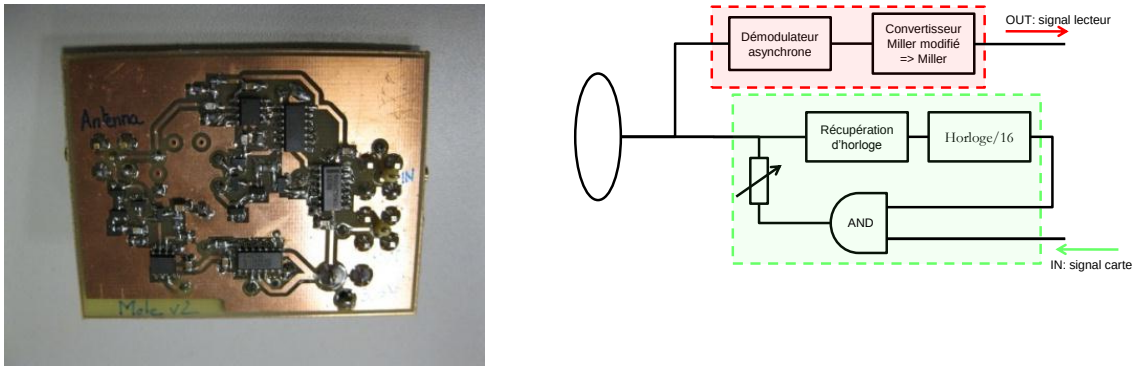


Figure II.47 – Le proxy : circuit et topologie du circuit électronique

a. Démodulation du signal lecteur

Le lecteur envoie des données codées en Miller modifié avec une modulation 100% ASK (OOK). Une telle modulation est caractérisée par des trous assez rapides dans le champ RF. La démodulation d'un tel signal est assez simple, car la modulation est en OOK ; un simple démodulateur asynchrone utilisant un détecteur d'enveloppe et un comparateur suffit pour démoduler le signal à 13.56MHz. Le signal démodulé obtenu a des niveaux hauts d'une durée entre 1 et 2 µs (les trous de la modulation Miller modifié) soit une fréquence du signal binaire entre 500 kHz et 1 MHz. Une telle bande passante est trop importante pour la plupart des systèmes de transmission sans fil que nous souhaitons utiliser entre le proxy et le môle. Le signal démodulé est donc décodé pour obtenir un signal en Miller caractérisé par un front (montant ou descendant) à chaque impulsion du signal en Miller modifié. La bande passante du signal obtenu est proche du débit binaire du signal soit 106 kHz. La figure II.48 montre la démodulation du signal en Miller modifié.

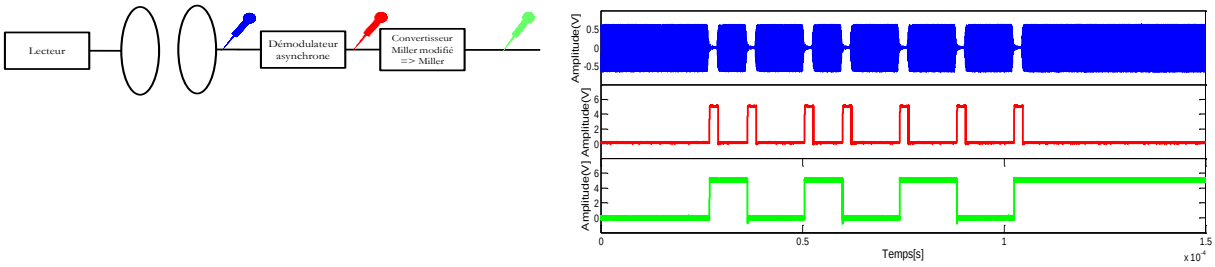


Figure II.48 – Proxy et signaux observés (voie montante)

b. Modulation du signal carte

Le signal entrant dans le proxy est un signal auparavant démodulé par le proxy et provenant de la carte de la victime. La forme du signal de la carte est appelée « modulation de charge », c'est-à-dire que la modification de la charge aux bornes de l'antenne de la carte va modifier de façon temporaire le couplage entre les deux antennes et désadapter l'antenne du lecteur. Ceci entraine une modification de la valeur efficace du courant dans l'antenne et peut être vu par ce lecteur comme une transmission de données. En ISO 14443-A, la carte utilise un codage Manchester avec sous-porteuse (figure II.49). Sans ajouter un canal de communication sans fil entre le proxy et le môle de façon à transmettre une horloge, il n'est pas possible de synchroniser les deux dispositifs. Il a donc été décidé que le môle transmettrait au proxy un signal directement codé en Manchester (horloge utilisée pour convertir le signal NRZ en Manchester). La récupération d'horloge permet de créer la sous-porteuse à 848 kHz. La modulation de charge est donc réalisée de façon synchrone avec le signal du lecteur comme si le proxy était une véritable carte sans contact. On observe avec une bobine de calibration proche de l'antenne lecteur que notre dispositif génère bien une modulation de charge propre, voir la figure II.50.

Figure II.49 – Codage Manchester

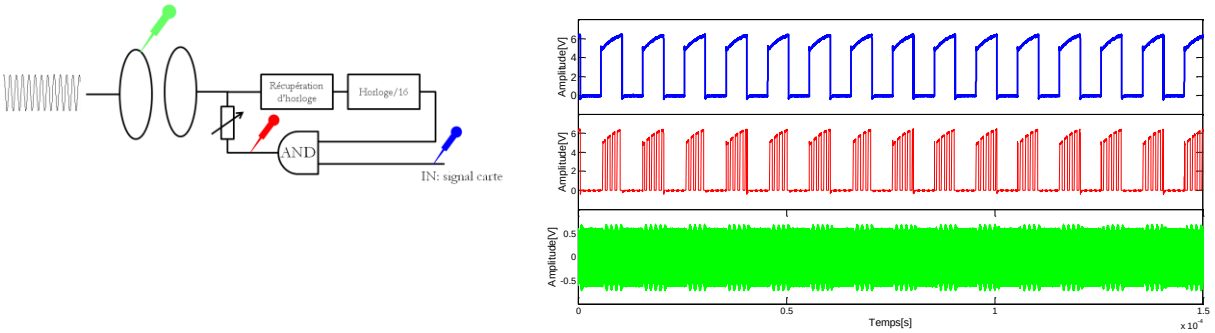


Figure II.50 – Proxy et signaux observés (voie descendante)

B. Le môle

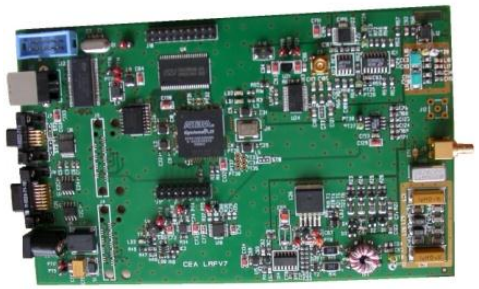


Figure II.51 – Le lecteur Lrfv7

Le môle est basé sur un lecteur de métrologie développé au CEA-Léti et utilisé dans la plupart des expérimentations que nous avons réalisées (figure II.51). Une partie en annexe explique le fonctionnement de cette carte. Ce dispositif possède un front-end RF permettant de moduler en amplitude n'importe quel signal dont la porteuse est à 13.56 MHz mais aussi de réceptionner et d'échantillonner un signal provenant de la modulation de charge d'une carte sans contact. Le cœur du môle est donc ce dispositif puisqu'il va nous permettre de retransmettre le signal

lecteur démodulé par le proxy mais aussi de réceptionner le signal de la carte de la victime de façon à le transmettre au môle. Le gros intérêt d'une carte dotée d'un FPGA par rapport à une carte purement analogique et qu'il est plus facile de dissocier la phase d'émission et la phase de réception et ainsi d'éviter les interférences en créant une liaison relais en half-duplex. Le traitement numérique des signaux est simplifié et le décodage et la mise en octets des trames sont possibles. Le signal provenant du proxy est directement traité par le FPGA du môle, il est recodé en Miller modifié et modulé en OOK. Le signal HF est alors amplifié et émis par l'antenne. La carte de la victime reconnait la trame de notre môle comme une trame venant d'un lecteur standard et répond en modulant sa charge. Ce signal est traité de façon analogique dans un premier temps puis échantillonné, démodulé et décodé par le FPGA.

C. La liaison wireless

Le proxy et le môle communiquent ensemble par le biais d'un système sans fil. Il est très difficile à l'heure actuelle de trouver des systèmes sans fil compatibles TTL avec un débit assez élevé. Nous souhaitons transmettre un signal numérique non lié à un protocole particulier comme le SPI. On trouve facilement des systèmes fonctionnant à 433 ou 868 MHz qui permettent par exemple de réaliser des systèmes de transmission bas débit en dessous de 50 kbit/s. Notre cahier des charges nous impose d'avoir un système sans fil dont le débit est supérieur à 212 kbits/s (la fréquence maximale du signal démodulé de la carte). Les seuls systèmes répondant à nos critères sont des puces utilisées dans les systèmes de transmission de vidéo/audio sans fil, voir la figure II.52.

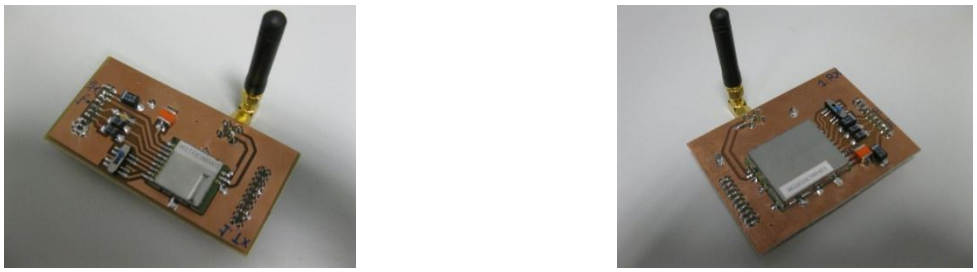


Figure II.52 – Systèmes de transmission TX et RX

Figure II.53 – Système complet

Les transmetteurs TX et récepteurs RX et ont été adaptés sur une même carte ce qui permet d'avoir un système global pour le proxy et pour le môle (figure II.53). Le système sans fil utilisé est disponible chez la plupart des fabricants d'électronique, deux transmetteurs et deux récepteurs sont nécessaires pour créer une liaison sans fil en full duplex. Elle sera utilisée en half-duplex car le lecteur n'émet jamais en même temps que la carte sans contact. Le gros avantage de ces modules est le choix entre 4 canaux de fréquence proche de 2.4 GHz, ce qui permet de limiter les interférences entre les deux couples émetteurs-récepteurs. Le prix de notre système sans fil est inférieur à 70€. Ces dispositifs possèdent 3 voies multiplexées mais seule la voie vidéo est utilisée car elle possède la plus grande bande passante (> 1MHz).

D. Système complet

Le relais complet est constitué des différents éléments que nous avons détaillés auparavant, voir la figure II.54). Chaque élément a un rôle important à jouer, mais l'objectif général est de réaliser un répéteur half-duplex entre le lecteur et la carte valide. La plupart des circuits ont été

réalisés en interne au CEA à partir d'éléments disponibles dans le commerce. Il est vrai que le môle et le proxy sont assez gros, mais l'important était de valider la réalisation d'un relais complexe dans un délai temporel assez court.

Figure II.54 – Système complet : système sans contact valide + attaque relais

Pour vérifier que l'ensemble était fonctionnel, nous avons utilisé un lecteur du commerce Inside Contactless compatible en particulier avec la norme ISO14443-A et une carte sans contact Mifare de NXP. Les résultats suivants montrent que l'on arrive sans problème à transmettre des signaux entre les deux dispositifs valides sans qu'ils s'aperçoivent de la présence du relais entre eux. La principale preuve de cette méconnaissance de l'attaque est que la carte répond au REQA du lecteur et que le lecteur comprend la réponse de la carte et déclenche le protocole d'anticollision, voir figure II.55.

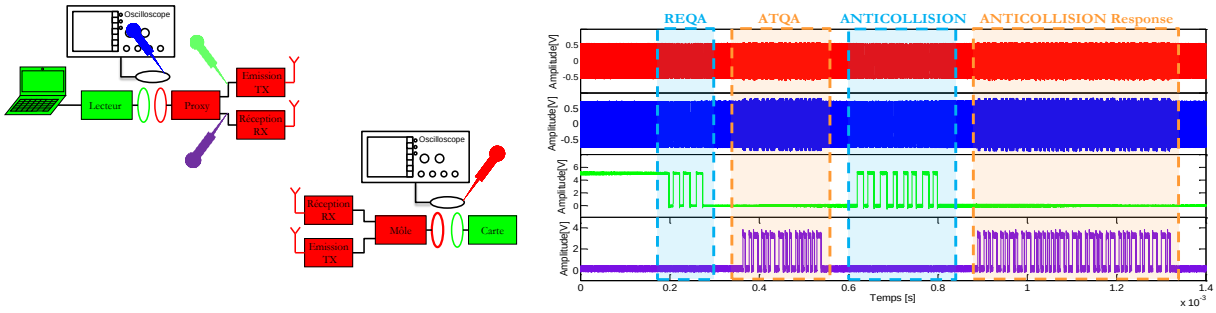


Figure II.55 – Signaux observés lors d'une attaque relais avec notre système

E. Caractéristiques de notre relais

a. Distance de fonctionnement

La « datasheet » des systèmes de transmission vidéo prévoit une distance de fonctionnement théorique d'environ 100 mètres. En pratique, il n'a pas été possible de tester sur une aussi grande distance. Cependant, en prenant compte les problèmes de propagation dans un bâtiment, la distance entre le proxy et le môle doit être de quelques dizaines de mètres. Cette distance est largement suffisante pour un attaquant. Basé sur des tests réalisés sur notre système relais, on obtient une distance maximale de 10 cm entre la carte et le môle mais aussi entre le proxy et le lecteur.

b. Délai introduit par le système

Ce relais introduit un délai plus important que les précédents puisque le signal est entièrement démodulé. Pas besoin d'utiliser la corrélation pour identifier un tel délai car celui-ci est visible à l'œil nu. Pour mesurer le délai sur la voie montante, nous allons mesurer le retard entre un front montant du signal lecteur au niveau du lecteur et au niveau de la carte lors d'un trou de champ RF. De même pour mesurer le délai introduit par la voie descendante de notre relais, nous mesurerons le retard entre un front montant de la sous-porteuse au niveau de la carte et au niveau du lecteur, voir figure II.56. Le délai trouvé aura une précision plus faible qu'en utilisant la corrélation mais l'objectif de ce relais n'était pas la rapidité, mais l'efficacité.

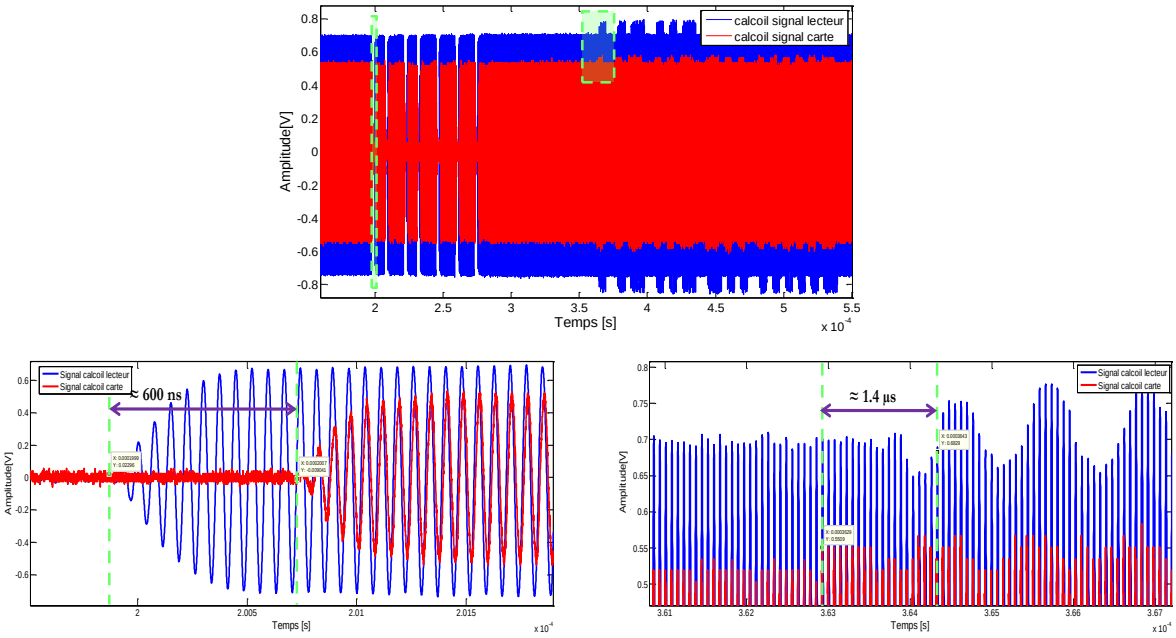


Figure II.56 – Délai de la voie montante et de la voie descendante

La voie montante de notre relais introduit un délai proche des 600 ns alors que la voie descendante approche les 1.4 µs. Cette différence de délai s'explique par la complexité de la chaine de réception du signal carte au niveau du môle.

Le chronogramme suivant est un résumé de tous les délais trouvés pour les différents relais, voir la figure II.57. Tous les relais que nous avons réalisés, même les plus sophistiqués introduisent un délai inférieur ou égal à 2 µs contre plus de 15 µs pour les relais de Hancke et Kasper.

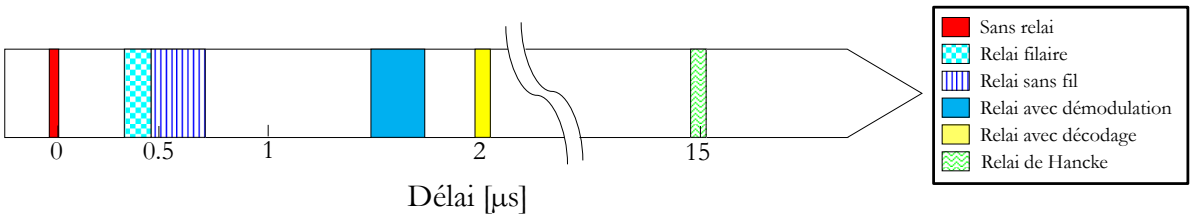


Figure II.57 – Délai introduit par les différents relais

F. Conclusion et améliorations possibles

Notre système permet de relayer n'importe quel message entre un lecteur et une carte valide sur plusieurs dizaines de mètres. Cependant, quelques améliorations peuvent permettre à notre système de devenir beaucoup plus complet. Une importante amélioration serait de décoder complètement l'information de façon à récupérer les octets transmis entre le lecteur et la carte. Ce travail a déjà été commencé mais n'a pas été terminé à temps. Cette amélioration pourrait permettre à la fois la modification des octets de façon à réaliser une attaque « man in the middle » mais aussi d'intégrer une communication sans fil basée sur le protocole SPI ou tout autre protocole. Il est aussi possible d'améliorer notre attaque en augmentant la distance d'activation de la carte de la victime. Actuellement, notre relais n'active une carte qu'à une dizaine de centimètres ce qui diminue le pouvoir de l'attaque. En utilisant les travaux de Kirschenbaum, il est possible d'augmenter cette distance jusqu'à une trentaine de centimètres [KIR2006].

Chapitre III. Contre-mesure basée sur la corrélation

Introduction du chapitre

Dans le chapitre « Réalisation d'attaques », différents relais ont été développés pour déterminer leurs principales caractéristiques temporelles. Dans cette partie, nous allons étudier la faisabilité d'une contre-mesure utilisant la corrélation pour détecter la présence de relais dans un système sans contact. Un relais introduit un retard plus ou moins faible dans les trames transmises entre un lecteur et une carte comme cela a été démontré dans le chapitre précédent. Ce délai est en partie dû au temps de propagation du signal dans l'air (quelques centaines de ps), au temps d'établissement du signal dans les antennes (dépendant du facteur de qualité de celles-ci) mais aussi au temps de traitement spécifique au relais. Ce retard introduit par le relais peut varier entre 200 ns et plus de 20 µs pour des relais sophistiqués. L'objectif de notre contre-mesure est la détermination de ce temps en se basant sur la corrélation, technique très connue en traitement du signal. Cette méthode est intégrée dans un protocole d'authentification permettant d'identifier la présence d'une carte valide en face du lecteur sans contact. L'algorithme de détection de relais a été implémenté sur un système sans contact d'expérimentation développé par une équipe du CEA-Léti. La résolution de notre solution est proche de 300 ns, ce qui nous permet de détecter la plupart des attaques relais.

PARTIE I. ETAT DE L'ART

1. Protocole de « Distance bounding » et détection d'attaques relais

Depuis la publication de l'article de G. Hancke étudiant la possibilité de détection d'attaques relais par la mesure de délais entre l'émission d'une requête par le lecteur et la réception de la réponse de la carte, de nombreux articles décrivant des protocoles ont été développés [HAN2005-B]. Nous allons analyser les faiblesses au niveau de la couche physique de tels protocoles et montrer que cette contre-mesure n'est pas envisageable dans le cas d'un système sans contact.

Un protocole de distance bounding permet de fixer une limite de distance entre deux dispositifs et permet ainsi de détecter la présence d'attaques relais. La carte doit prouver au lecteur qu'elle est à proximité de lui, on l'appellera « prouveur ». Le lecteur, lui, vérifie cette proximité, il est appelé « vérifieur ». Ces protocoles sont le plus souvent divisés en 3 phases. La première phase est une phase de préparation, les deux parties s'échangent certains secrets qui vont être nécessaires pour la seconde phase. Cette phase est un échange très rapide de bits entre le « prouveur » et le « vérifieur » de façon à vérifier que la carte est à proximité du lecteur. Le « vérifieur » mesure donc le temps entre l'émission de sa requête et la réception de la réponse du « prouveur ». Ce temps permet de déterminer en théorie le temps introduit par la propagation du signal dans l'air et en déduire la distance entre les deux entités communicantes à partir de la vitesse de propagation du signal. La troisième phase est une phase d'authentification et de vérification. Le vérifieur analyse les réponses envoyées pendant la deuxième phase. Il en déduit si c'est la carte qui a effectivement répondu et ensuite calcule la distance séparant le lecteur et la carte à partir des temps trouvés pendant la deuxième phase. Il peut alors conclure sur la présence d'un relais. La figure III-1 présente le protocole développé par Hancke et Kuhn.

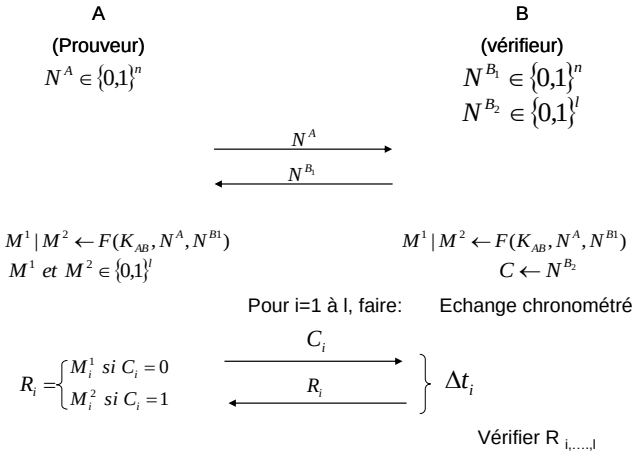


Figure III-1 – Protocole distance bounding par Hancke (2005)

On retrouve dans ce protocole les trois phases précédentes. Pendant la phase de préparation, le vérifieur génère deux nombres aléatoires N^{B_1}et N^{B_2} respectivement de longueur n et l. Il transmet ensuite N^{B_1} au « prouveur ». Ce dernier génère dans le même temps un autre nombre aléatoire N^A qu'il transmet au « vérifieur ». Le « prouveur » et le « vérifieur » calculent alors tous les deux $F(K_{AB}, N^A, N^{B_1})$ à partir de la fonction pseudo-aléatoire F. Ils divisent le résultat obtenu en deux suites de bits soit M^1 et M^2. De son côté, le « vérifieur » génère une autre suite de bits C à partir de N^{B_2}.

Pendant la phase d'échange chronométrée, l challenges sont envoyés au « prouveur » par le « vérifieur ». Chacun de ces i challenges correspond à une valeur de C_i, soit un bit à 1 ou à 0. Le « prouveur » doit alors répondre un bit dépendant de la valeur de C_i. Si C_i=0, le « prouveur » envoie M_i^1 et si C_i=0, le « prouveur » envoie M_i^2. Pour chacun de ces challenges, le « vérifieur » mesure le temps entre l'envoi de la requête et la réception de la réponse.

Pendant la phase dite de vérification ou d'authentification, le « vérifieur » vérifie les bits envoyés par le « prouveur » pendant la phase d'échange.

Bien que ce protocole ne résiste pas à l'attaque « terrorist fraud », sa fiabilité cryptographique est particulièrement intéressante vis-à-vis d'une attaque relais. En effet, une simple authentification ne suffit pas à déterminer la présence d'un relais ; seul le délai introduit par ce relais peut permettre de le détecter.

Cependant, la fiabilité de cette contre-mesure ne dépend pas seulement de la qualité du protocole, mais aussi et surtout de la couche physique du système. Le canal de communication utilisé lors de la phase d'échange a une importance fondamentale sur la mesure du temps de propagation du signal. Bien que le nombre de propositions concernant ces protocoles ne fasse que croître, la plupart des rédacteurs se contentent d'améliorer le protocole sans donner d'indication sur son implémentation. De nombreux articles vantent le coût, la complexité ou la fiabilité de leur protocole sans penser à l'implémentation d'une telle contre-mesure sur un système sans contact. Nous allons montrer l'importance d'une telle réflexion avant de nouvelles recherches sur ces protocoles.

La mesure de distance par le biais d'ondes électromagnétiques ou acoustiques existe depuis de nombreuses années. Chacun de ces supports d'informations possède des caractéristiques précises permettant de mesurer la distance entre un émetteur et un récepteur.

La relation liant la résolution en distance r en mètres à la bande passante d'un signal B en Hertz et à la célérité de l'onde dans l'air c en mètres/seconde est la suivante [HAN2005-B]:

$$r = \frac{c}{B} \qquad \text{(III-1)}$$

La résolution d'une onde dépend donc du rapport entre la bande passante du signal de ce système et la célérité de l'onde portant ce signal.

Ainsi, un système de mesure utilisant les ondes ultrasons dont la célérité dans l'air est de 343 m/s et la bande passante est de 15 kHz (bande passante observée sur des produits utilisant les ultrasons) permet d'obtenir une résolution de 2.3 cm.

De la même façon, un système utilisant les ondes électromagnétiques dont la célérité est proche de celle de la lumière dans l'air permet d'obtenir une résolution de 354 mètres pour un système HF dont la bande passante est de 848 kHz.

La bande passante d'un système UWB correspond à 20-25% de la fréquence centrale. On peut donc obtenir une résolution de 1,6 m pour un système utilisant des pulses de bande passante 250 MHz (fréquence centrale = 1 GHz). La résolution minimale d'une quinzaine de centimètres est atteinte lorsque la fréquence centrale du système est proche des 7 GHz.

Pour un système utilisant les ondes électromagnétiques, il est nécessaire de préciser qu'une erreur d'une nanoseconde sur le résultat de temps trouvé induit une erreur de 30 cm dans la valeur de distance trouvée (valeur supérieure à la distance de fonctionnement des systèmes sans contact).

Nous allons maintenant montrer que les systèmes proposés à base d'UWB ou d'ondes HF ne permettent pas de trouver une distance précise entre l'émetteur et le récepteur.

La figure III-2 montre le système de transmission de données entre un « prouveur » et un « vérifieur ». Le « vérifieur » envoie une requête au « prouveur ». Cette requête peut être un simple bit comme dans le système Hancke ou une trame plus complète. Le bit est cependant privilégié dans le cas d'un système de mesure de retards. Dans le même temps, le « vérifieur » démarre un compteur de façon à mesurer le temps avant le retour de la réponse du « prouveur ». Cette requête envoyée par le « vérifieur » doit ensuite être modulée par le bloc « TX vm » avant injection dans l'antenne d'émission (magnétique ou électrique selon le canal de communication utilisé).

Le signal est récupéré sur l'antenne du « prouveur », démodulé avec le bloc « RX vm » de façon à déterminer la requête du « vérifieur ». En général, la requête n'a pas besoin d'être décodée pour ne pas ajouter des délais supplémentaires. A partir de la requête reçue, le « prouveur » déduit la réponse à envoyer, cette réponse est donc modulée avec le bloc « TX vr » (modulation de charge pour un canal de communication sans contact par exemple) et injectée dans l'antenne. Le « vérifieur » reçoit alors la réponse du « prouveur », la démodule avec le bloc « RX vr » et stoppe dans le même temps le compteur. L'interprétation de la réponse du « prouveur » est réalisée généralement après la phase d'échange chronométrée.

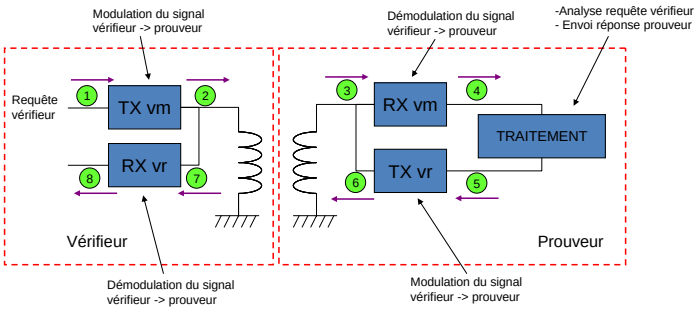


Figure III-2 – Système de transmission entre le prouveur et le vérifieur

Le tableau III-1 donne les différents temps induits par un système utilisant les ondes radios et la dénomination de chacune de ces valeurs.

Tableau III-1 – Définition des différents temps liés au transfert d'informations

t_E	Temps d'établissement des signaux dans les antennes utilisées pour l'émission et la réception (on choisit le même pour toutes les antennes même si ce n'est pas vraiment le cas)
t_P	Temps de propagation de l'onde électromagnétique
t_{CTX}	Temps nécessaire à la modulation du signal « prouveur » pour envoi vers le « vérifieur »
t_{CRX}	Temps nécessaire à la démodulation du signal « vérifieur » par le « prouveur »
t_{LTX}	Temps nécessaire à la modulation du signal « vérifieur » pour envoi vers le « prouveur »
t_{LRX}	Temps nécessaire à la démodulation du signal « prouveur » par le « vérifieur »
t_T	Temps de traitement du « prouveur » pour calculer la réponse à envoyer
t_D	Délai mesuré entre la requête du « vérifieur » et la réception de la réponse du « prouveur »

Chaque modification du signal introduit un temps correspondant aux différentes phases de traitement du signal (figure III-3 et tableau I-1). La modulation et la démodulation du signal ajoutent des temps de latence non négligeables et différents selon les formats de modulation et de démodulation utilisés. Dans le domaine du sans contact, la voie retour n'est pas modulée de la même façon que la voie aller ; les délais introduits sont donc différents. Le temps d'établissement du signal dans les antennes est non nul, il dépend avant tout de la fréquence porteuse et des paramètres de l'antenne (la bande passante, …)

Le temps de propagation du signal dans l'air est très faible puisqu'une onde électromagnétique a une célérité dans l'air proche de celle de la lumière. Dans un système sans contact classique, ce temps de propagation est proche de 300 ps si on considère que le lecteur et la carte sont à 10 cm l'un de l'autre.

Le temps de traitement de l'information par le « prouveur » peut être très rapide, mais peut varier légèrement selon les données transitant comme le précise G. Hancke [HAN2008-C]. Une porte logique NOT possède un temps de latence dépendant de la valeur mise en entrée. Le temps de traitement n'est donc pas vraiment fixe et une erreur de quelques ns peut avoir de grosses conséquences sur la mesure de distance.

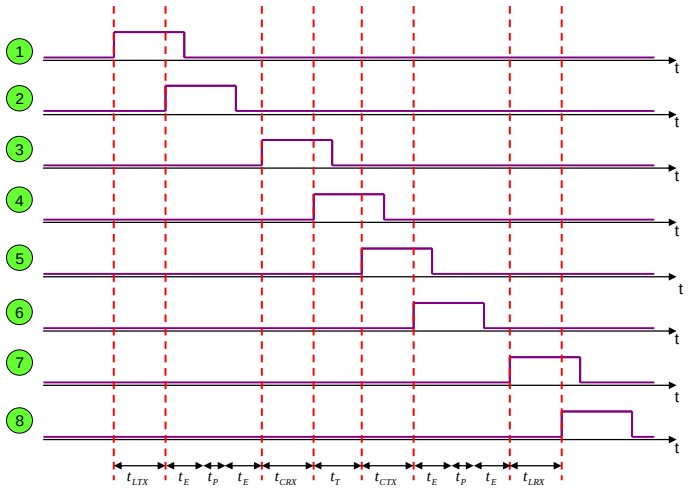


Figure III-3 – Chronogramme de la contre-mesure utilisant un canal de communication sans fil ou sans contact

En ajoutant tous les délais introduits par le système, on obtient l'équation III-2.

$$t_D = t_{LTX} + t_{LRX} + t_{CTX} + t_{CRX} + 2(t_P + 2t_E) + t_T \quad \text{(III-2)}$$

Le temps de propagation t_P peut donc être calculé par l'équation III-3.

$$t_P = \frac{t_D - (t_{LTX} + t_{LRX} + t_{CTX} + t_{CRX} + 4t_E + t_T)}{2} \quad \text{(III-3)}$$

Les protocoles de distance bounding sont basés sur l'hypothèse que les temps de traitement du signal est négligeable par rapport au temps de propagation du signal ce qui n'est pas le cas dans un système sans contact, voir l'équation III-4.

$$t_P >> \frac{(t_{LTX} + t_{LRX} + t_{CTX} + t_{CRX} + 4t_E + t_T)}{2} \quad \text{(III-4)}$$

Il est possible de mettre en évidence la faiblesse d'une telle solution que ce soit en utilisant un canal de communication sans contact ou UWB.

A. Mise en place d'un protocole distance bounding en utilisant le même canal de communication (canal HF)

Il n'est pas possible d'utiliser un canal de communication HF pour mesurer une distance très faible entre un émetteur et un récepteur. Tout d'abord, la résolution en distance d'un signal à 13,56 MHz est bien trop faible puisque proche des 400 mètres. De plus les temps d'établissement dans les antennes, les temps de modulation et de démodulation du signal sont trop longs pour mesurer des retards faibles.

B. Mise en place d'un protocole distance bounding utilisant l'UWB

L'utilisation de l'UWB sur un système sans contact HF est impensable. Les contraintes matérielles sont nombreuses comme la modification de toute la partie front-end RF. Le signal UWB est un signal large bande et implique l'utilisation d'antennes électriques et de blocs de modulation et démodulation adéquats. Toutes ces modifications ajoutent énormément de complexité à notre système: deux antennes, deux front-end RF, des entrées et sorties supplémentaires en plus sur la puce du système. Ces modifications matérielles ajoutent un coût important pour une simple carte sans contact.

La résolution en distance demande l'utilisation de fréquences très élevées et une nanoseconde de différence dans le résultat trouvé peut induire une erreur d'une trentaine de centimètres, ce qui reste énorme.

Hancke et Kuhn font partie des quelques auteurs qui ont développés la partie couche physique du système. Leur conclusion est assez proche de la nôtre ; ils insistent sur le fait que le canal de communication HF présente des vulnérabilités temporelles ne permettant pas d'utiliser des protocoles de distance bounding. Dans le même temps, ils montrent que l'utilisation d'un canal UWB pourrait être possible, mais son implémentation incomplète ne permet pas de valider la fiabilité d'une telle contre-mesure.

Rasmussen et Capkun ont aussi montré qu'il était possible d'implémenter l'électronique de comparaison de signaux pour les protocoles de distance bounding [KAS2010]. L'objectif de leurs travaux est de montrer qu'il est possible de développer une structure électronique permettant de mesurer une distance entre le « prouveur » et le « vérifieur » avec une précision de 15 cm. Cette distance nécessite une précision temporelle d'environ 1 ns. Pour garder un temps de traitement de l'information très court, le « prouveur » ne peut pas démoduler les données, car ce traitement nécessite généralement plus de 50 ns. Il n'est donc pas possible d'utiliser un protocole de distance bounding basé sur une opération XOR car elle exige une démodulation du signal. La concaténation de signaux représente une bonne solution puisqu'aucune démodulation n'est

nécessaire. Comme on peut le voir sur la figure III-4, la multiplication du challenge par f_Δ permet d'obtenir deux bandes de fréquences ; le « prouveur » doit alors choisir la bonne bande de fréquences à renvoyer au « vérifieur ». Leur solution a été entièrement développée à partir de circuits RF, comme le montre la figure III-5. Ils ont ensuite réalisé différentes mesures et ont démontré que leur système permettait de recevoir, de traiter et de transmettre une information en moins d'une ns.

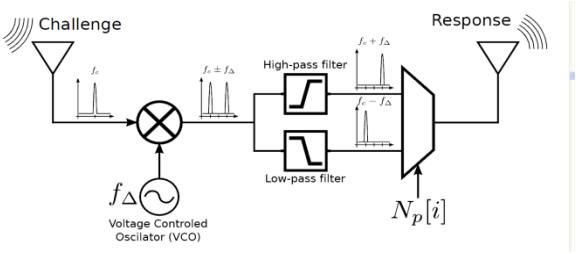


Figure III-4 – Synoptique de la structure du « prouveur »

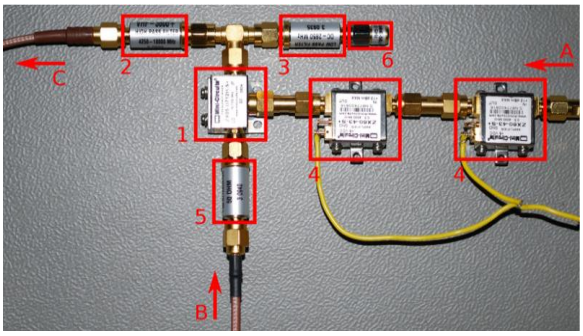


Figure III-5 – Prototype du « prouveur » : Le circuit 1 représente le mixer. Le signal du « vérifieur » arrive par A, B est l'oscillateur de fréquence f_Δ Les circuits 2 et 3 sont les filtres permettant de choisir l'une ou l'autre des deux bandes de fréquences

Leur solution est particulièrement intéressante. Bien que leur système ne soit pas vraiment complet (choix manuel de la bande de fréquence au niveau du « prouveur », traitement de l'information par le « vérifieur »), leur système est fonctionnel et représente une grande avancée sur la réalisation de protocoles de distance bounding. Bien entendu, un tel système ne fonctionne qu'avec des fréquences très élevées et ne peut pas être implémenté sur un système sans contact.

2. La corrélation croisée

Cette fonction mathématique permet de quantifier la ressemblance entre deux signaux, voir l'équation III-5.

$$Rxy(k) = \sum_{n=-\infty}^{\infty} x(n+k).y(n) = \sum_{n=-\infty}^{\infty} x(n).y(n+k) \qquad \text{(III-5)}$$

Soit x et y deux fonctions du temps, l'objectif de la corrélation est de mesurer de combien d'échantillons le signal x doit être avancé ou reculé par rapport à y de façon à ce que les deux signaux aient le plus de ressemblance. Pour réaliser le calcul, pour chaque déplacement de y d'un échantillon, on calcule le résultat de la multiplication des deux signaux que l'on veut comparer échantillon par échantillon. Cette valeur est maximale lorsque les deux signaux sont les plus semblables ; le décalage trouvé entre les deux signaux correspond au retard.

Les applications utilisant la fonction corrélation sont nombreuses :

A. Radars pour l'anticollision de véhicules

Dans cette application, le radar émet une onde vers la cible ; celle-ci renvoie un écho. L'onde émise peut être une simple impulsion ou un signal modulé. On traite l'écho pour obtenir des informations.

Le radar présenté dans l'article [MEN1999] est le radar à corrélation.

Ce radar utilise la corrélation pour extraire les informations du signal de retour. Le signal HF est modulé par une séquence pseudo aléatoire (obtenu à partir de registre à décalages).

On calcule la fonction d'intercorrélation entre le signal obtenu en réception (après démodulation et filtrage) et le code utilisé en émission. Le résultat de cette intercorrélation permet de définir un retard entre les deux signaux : ce retard permet de déterminer la distance entre l'émetteur d'ondes et l'objet.

B. Sonars

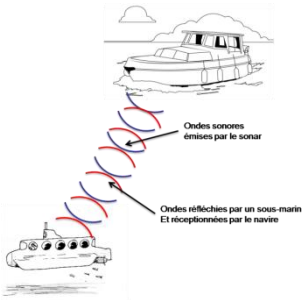


Figure III-6 – Les sonars

Les sonars, voir la figure III-6, sont très proches des systèmes radars, mais utilisés pour le milieu marin et utilisent donc les ondes acoustiques. Le sonar est un système de détection d'objets basé sur la réflexion d'ondes sonores. Le système sonar émet des ondes ultrasonores grâce à un appareil émetteur et reçoit ces mêmes ondes réfléchies par la coque du sous-marin à l'aide d'un récepteur sensible aux ultrasons.

La chaîne de traitement placée derrière ce récepteur calcule la corrélation entre le signal envoyé et le signal reçu pour en déduire le délai et en conclure sur la position du sous-marin.

PARTIE II. CORRELATION DE SIGNAUX MODULES

Pour obtenir une valeur de corrélation fiable et précise, le signal x doit présenter des caractéristiques qui vont être étudiées dans cette section. Ces caractéristiques ont été évaluées au fur et à mesure des simulations et des expériences réalisées. On s'intéresse ici uniquement à l'étude d'un signal modulé en amplitude, nous verrons par la suite qu'il est possible de travailler avec un signal modulé en phase dans certains cas que nous présenterons.

1. Importance du niveau de porteuse du signal

Dans le domaine du sans contact, les normes existantes utilisent généralement des signaux modulés en amplitude possédant deux niveaux d'amplitude (niveau modulé et niveau non modulé), voir la figure III-7.

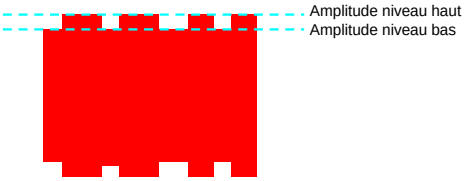


Figure III-7 – Niveau d'amplitude d'une modulation d'amplitude

L'objectif de cette partie est la mise en évidence d'un phénomène lors de la corrélation de signaux modulés en amplitude. La comparaison de deux signaux identiques au niveau codage, information utile (correspondant à la séquence à corréler) et fréquence porteuse permet de montrer que certaines précautions doivent être prises lors du calcul de la corrélation et du choix des signaux. Lors du calcul de corrélation, une partie du signal correspond au signal à comparer appelé signal utile ; une autre partie correspond à des échantillons supplémentaires permettant de faire glisser l'un des deux signaux échantillon par échantillon pour calculer toutes les positions décalées dans le temps de ce signal par rapport à l'autre. L'objectif est de montrer que l'amplitude des signaux à proximité de la séquence à corréler a une importance dans le calcul de la corrélation. Nous comparons deux signaux présentant le même signal utile, mais une amplitude du signal à proximité de la séquence utile différente. La figure III-8 montre les deux signaux à comparer : le premier est le signal rouge (hachures non comprises) qui montre que le signal utile à

une amplitude plus élevée que le signal autour de la séquence à corréler. Le deuxième signal est le signal rouge avec les hachures ; le signal permettant le glissement du signal a une amplitude maximale plus élevée ou égale à l'amplitude maximale du signal à corréler.

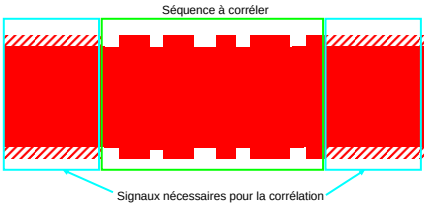


Figure III-8 – Séquence à corréler et signaux proches

Ces deux signaux ont été simulés sous Matlab, voir la figure III-9, et corrélés avec leur copie retardée dans le temps. Le premier signal sera le signal A et le deuxième B.

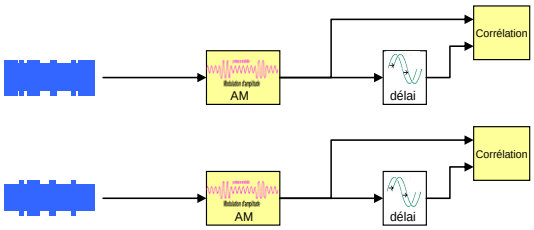


Figure III-9 – Corrélation de signaux présentant des niveaux de porteuse différents

Après modulation, les deux signaux en sortie sont retardés d'une valeur de 36.9 ns correspond à une demi-période à la fréquence de la porteuse utilisée en sans contact. L'objectif de la corrélation est donc de retrouver ce délai entre le signal et sa copie retardée dans le temps. Le délai fixé pour notre simulation est de 36.9 ns correspondant à une demi-période de la porteuse de notre signal à 13.56 MHz. Le signal est échantillonné à 100 MS/s ce qui permet une résolution théorique de 10 ns. La corrélation du signal avec sa copie décalée doit permettre de trouver pour une valeur de délai de 36.9 ns un retard de 40 ns ou -40 ns (selon le calcul de la corrélation).

Le signal A implémenté sous Matlab correspond à la figure III-10 ; le résultat de la corrélation montre un pic de corrélation à -40 ns qui ne correspond cependant pas au maximum du signal de corrélation. En effet, on remarque que plus notre signal est décalé dans le temps et plus la valeur de corrélation augmente, et ce, jusqu'à dépasser l'amplitude du pic de corrélation. Ceci s'explique à cause de l'amplitude du signal de la porteuse permettant de décaler le signal échantillon par échantillon. Nous reviendrons sur cette étude après analyse du signal B.

Le retard trouvé par la fonction mathématique de corrélation est de -198 µs. Ce retard est très éloigné du retard attendu.

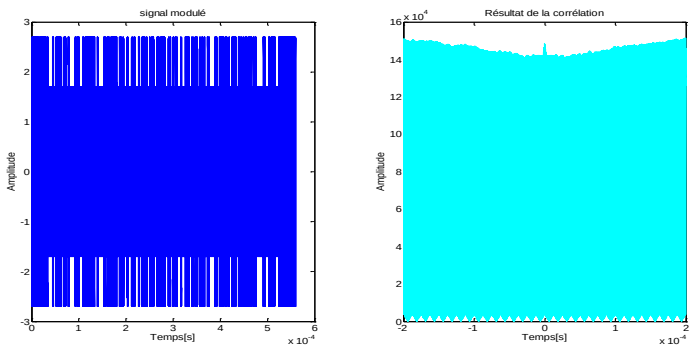


Figure III-10 – Signal corrélé A et le signal corrélé avec sa copie retardée dans le temps

Le deuxième signal implémenté sous Matlab correspond à la figure III-11, le résultat de la corrélation montre un pic de corrélation à -40 ns et correspond bien au maximum du signal de corrélation. De plus, on remarque que plus notre signal est décalé et plus le signal de corrélation diminue.

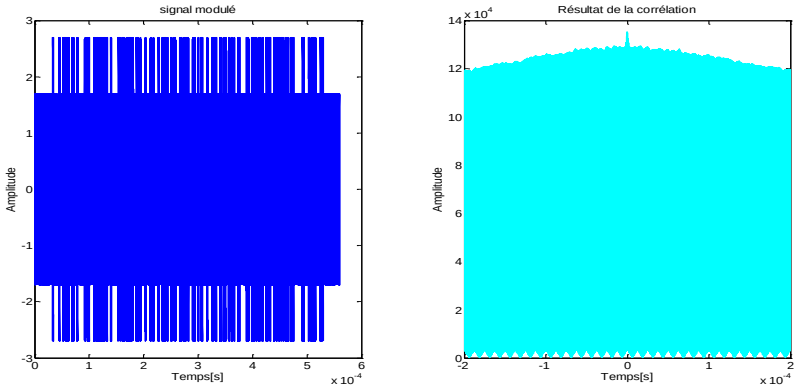


Figure III-11 – Signal corrélé B et le signal corrélé avec sa copie retardée dans le temps

Ce test a permis de montrer l'influence de l'amplitude du signal de la porteuse. Nous allons expliquer par des exemples simples ce phénomène.

Soit A (figure III-12) et B (figure III-13) deux signaux ; le signal A est un signal modulé en amplitude et le signal B est le signal de la porteuse non modulée.

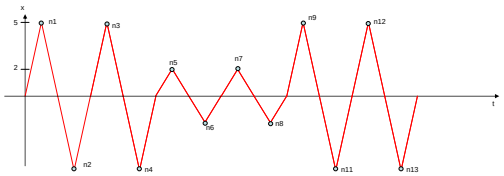


Figure III-12 – Signal A d'amplitude maximale 5

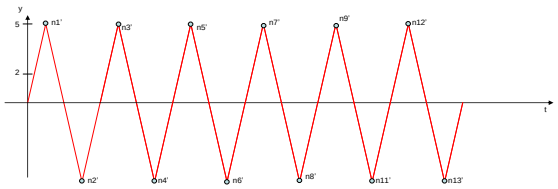


Figure III-13 – Signal B d'amplitude maximale 5

On montre que l'intercorrélation entre ces deux signaux possède un pic de corrélation plus élevé que l'auto corrélation du premier signal. L'intercorrélation ne permet pas de voir la ressemblance entre deux signaux.

Valeur de l'auto corrélation de A :

$$auto\_corr(A) = n1*n1 + n2*n2 + n3*n3 + n4*n4 + n5*n5 + ... + n13*n13 = 216$$

Valeur de l'inter corrélation de A et B :

$$corr(A,B) = n1*n1' + n2*n2' + n3*n3' + n4*n4' + n5*n5' + ... + n13*n13' = 300$$

Par contre, si le signal codé sous porteuse est supérieur à l'amplitude de la porteuse, soit A (figure III-14) et B (figure III-15) :

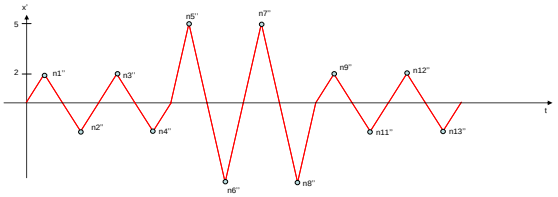


Figure III-14 – Signal A d'amplitude maximale 5

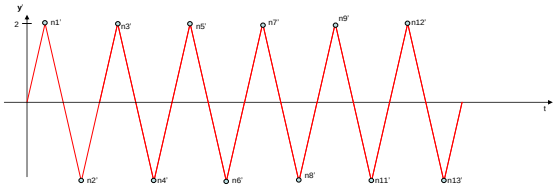


Figure III-15 – Signal B d'amplitude maximale 2

Valeur de l'auto corrélation de A :

$$auto\_corr(A) = n1''*n1''+n2''*n2''+n3''*n3''+n4''*n4''+n5''*n5''+....+n13''*n13''=132$$

Valeur de l'inter corrélation de x et y :

$$corr(A,B) = n1''*n1'+n2''*n2'+n3''*n3'+n4''*n4'+n5''*n5'+....+n13''*n13'=48$$

Le résultat ne laisse pas de doute, le signal utile doit avoir une amplitude maximum supérieure à la porteuse s'il l'on veut que la corrélation donne des résultats cohérents

2. Auto corrélation de différents types de codage

L'objectif est d'étudier le codage du signal qui sera modulé pour ensuite être corrélé. On cherche à obtenir un signal dont la fonction d'auto corrélation présente les caractéristiques les plus intéressantes. Ces caractéristiques sont le pic de corrélation (largeur et amplitude) et l'amplitude du reste de la corrélation.

Les codages étudiés sont des codages utilisés dans les normes du sans contact. Tous ces codages sont des codages à deux niveaux : niveau bas et niveau haut.

A. Les codages

a. Le codage NRZ

Ce codage est le plus simple puisqu'il est directement déduit de la séquence binaire. Un état logique '1' est représenté par un état haut du signal et un état logique '0' par un état bas du signal.

b. Le codage RZ (retour à zéro)

Ce codage est proche du codage NRZ mais le signal retourne à zéro pendant une demi-période d'horloge. On a donc un état logique '1' représenté par un niveau haut pendant une demi-période d'horloge suivi d'une demi-période d'horloge à l'état bas. Un état logique '0' est représenté par un état bas.

c. Le codage Miller modifié

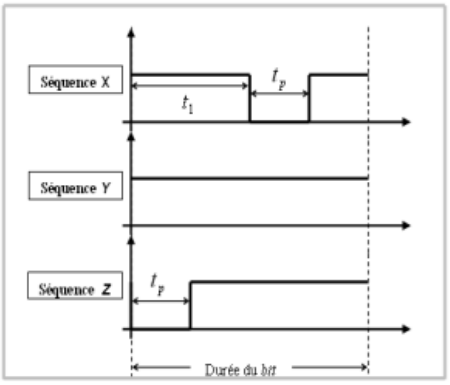


Figure III-16 – Séquences du codage Miller

Ce codage, voir la figure III-16, est plus complexe que les autres puisque son état présent dépend en partie de la valeur précédente de la séquence binaire, on a donc un effet mémoire dans le codage.

- Pour coder un '1' logique : la séquence X est utilisée, voir figure III-16.
- Pour coder un '0' logique : la séquence Y est utilisée sauf s'il y a deux ou plusieurs « 0 » qui se suivent, la séquence Y sera alors utilisée à partir du deuxième '0', voir figure III-16.

d. Le codage de position 1 sur 4

Ce codage permet de coder deux bits dans une même période de temps. Pour cela, on transmet une impulsion de durée un quart de période. Selon la position de cette impulsion dans la période de temps, on peut savoir la valeur des bits transmis. Pour transmettre deux bits, on a 4 possibilités de valeurs ce qui induit 4 positions pour l'impulsion.

e. Le codage Manchester

Chaque état logique est représenté par un changement d'état du signal à la moitié de la période de l'horloge. Un état '0' est donc représenté par une transition du niveau bas vers le niveau haut et l'état '1' d'une transition du niveau haut vers le niveau bas.

f. Le codage Manchester sous porteuse

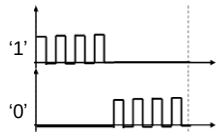


Figure III-17 – Codage Manchester sous porteuse

Le codage Manchester sous porteuse, voir la figure III-17, comme son nom l'indique est une variante du codage Manchester. Pendant une moitié du bit à transmettre, le signal est en modulation OOK à une fréquence appelée fréquence sous porteuse, multiple de la fréquence porteuse. L'autre moitié du bit est à 0.

B. Implémentation sous Matlab

Ces différents codages ont été implémentés sous Matlab de façon à valider le choix du codage de la séquence à corréler. La figure III-18 montre une même séquence pour les différents codages.

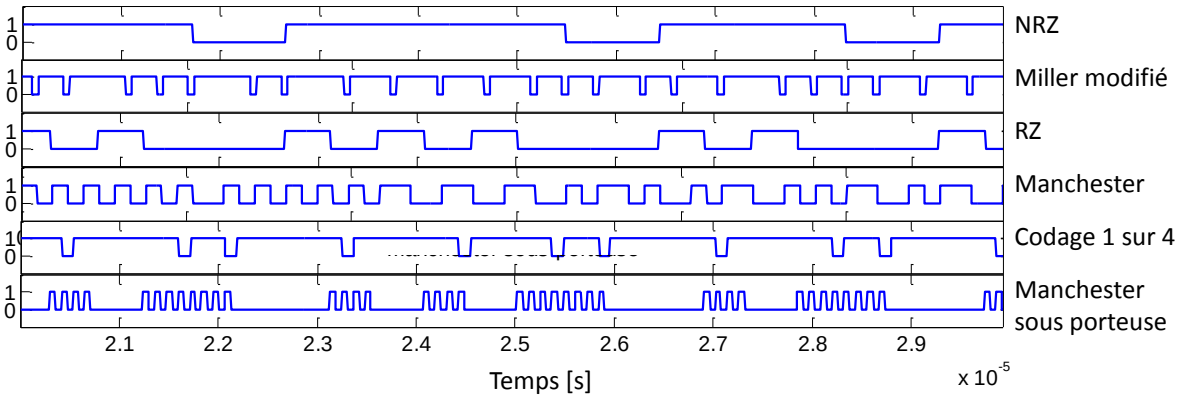


Figure III-18 – Séquences codées

Les différents signaux codés sont alors corrélés de façon à obtenir la fonction d'autocorrélation de tous ces signaux. Il est alors possible de tous les comparer selon leurs caractéristiques. La figure III-19 montre la fonction d'autocorrélation de tous ces signaux. Un codage se distingue rapidement par rapport aux autres : le codage NRZ. Il présente en effet un pic de corrélation dont l'amplitude est relativement plus importante que l'amplitude sans détection du signal ce qui est très intéressant dans notre cas. Cependant, la largeur de la base de ce pic n'est pas la plus faible, mais cela n'a pas d'importance car l'objectif de cette corrélation n'est pas de comparer plusieurs pics de corrélation.

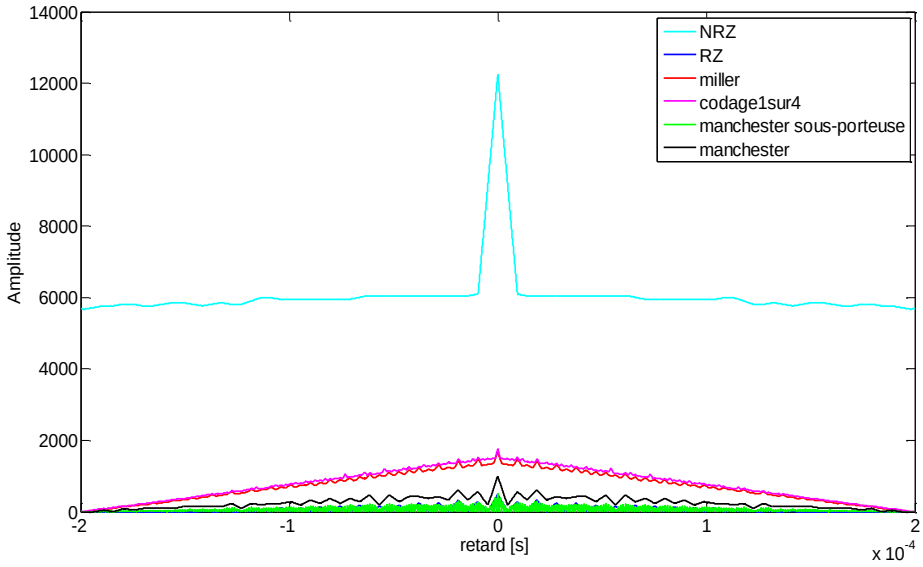


Figure III-19 – Fonction d'autocorrélation des différents signaux

3. Techniques de traitement du signal avant corrélation

Certaines phases de traitement sont nécessaires lors de l'implémentation de la fonction de corrélation. Ces techniques ont été utilisées lors:

- Des tests réalisés avant l'implémentation de la solution pour déterminer des délais avec une meilleure précision
- Des tests Matlab implémentant le système de mesures de délais
- De l'implémentation de la solution sur un composant programmable FPGA

A. Echantillonnage du signal pour traitement sur Matlab

L'objectif est de réaliser un échantillonnage permettant de numériser les extremums du signal. Ce type de traitement correspond à une recherche des extrémums du signal qui est implémenté en VHDL dans le FPGA. Dans l'objectif de se placer dans une méthodologie identique au système implémenté, on réalise la même implémentation sur Matlab pour travailler sur des signaux enregistrés sur l'oscilloscope. Ces signaux sont auparavant échantillonnés à 5GS/s par l'oscilloscope.

Les résultats obtenus sur cette recherche de maximum sont représentés sur la figure III-20.

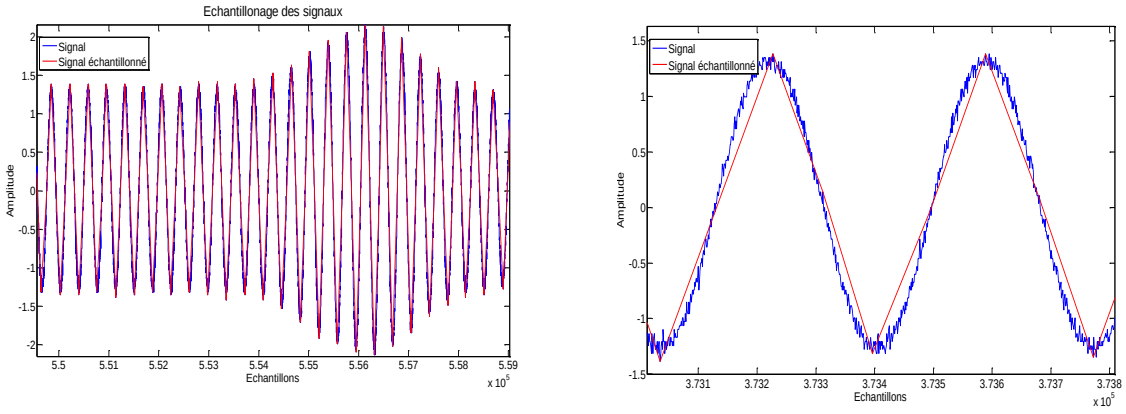


Figure III-20 – Echantillonnage du signal

On remarque que les extremums identifiés par cet échantillonnage sont parfois décalés par rapport à ce que l'on devrait trouver. Ce retard est principalement introduit par le bruit dans le système sans contact et par la résolution de l'oscilloscope. Une amélioration de cette solution est de calculer la moyenne des n maximums (n =10 par exemple) à chaque pic de la sinusoïde de fréquence 13.56 MHz, de regarder ensuite la position temporelle de ces maximums et d'en déduire la position temporelle du maximum et son amplitude. Cependant, la solution de base est suffisante pour les tests réalisés.

B. Démodulation par position des extremums sur Matlab

L'objectif de cette méthode est la recherche des pics correspondants à la modulation d'amplitude. Cette méthode est assez simple à réaliser sous Matlab puisque notre signal est enregistré. Le décalage temporel entre ces extremums va permettre d'obtenir une valeur assez précise du retard introduit par un relais.

La mesure du retard s'effectue en plusieurs étapes :

- La première étape consiste à échantillonner les signaux par exemple par la méthode introduite précédemment
- La deuxième étape consiste à mettre en forme notre signal
- La troisième étape est le calcul de la corrélation

La deuxième étape consiste ici à analyser la position temporelle des pics de modulation d'amplitude (modulation de charge par exemple). La figure III-21 permet de comprendre comment est réalisée la recherche de ces pics de modulation et comment est traitée l'information qu'ils apportent. Lorsqu'un extremum est détecté, le signal de sortie passe à 1, et à 0 lorsqu'il n'y pas présence d'un extremum.

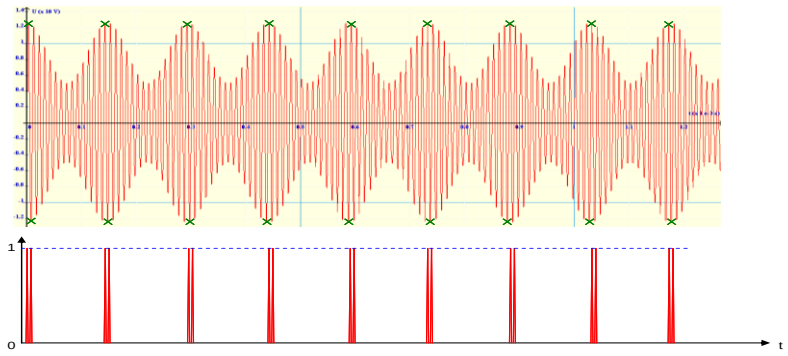


Figure III-21 – recherche des extremums

Deux signaux de sortie sont donc obtenus après traitement du signal côté carte et du signal côté lecteur. Ces deux signaux sont binaires ; ils comportent des pics d'amplitude 1, de largeur une demi-période de la porteuse soit 36.87 ns. Il est donc plus simple de faire une corrélation sur un tel signal que sur un signal modulé tel qu'il était avant traitement.

Avantages et inconvénients de la méthode :

Le principal inconvénient de cette méthode est que l'on perd en précision au niveau du retard introduit par le relais. Notre méthode revient à démoduler le signal, mais sans le traitement complexe que représente cette démodulation. Ce retard est principalement dû à un filtre permettant d'obtenir les pics de modulation.

Cette solution présente un vrai potentiel puisqu'elle est assez simple à implémenter. Un de ces avantages dans le cadre de la contre-mesure à l'attaque relais est que la génération et l'enregistrement d'un signal binaire sont beaucoup plus simples que pour un signal modulé.

Un autre avantage est que le codage et la séquence choisis ne sont pas importants, il faudra cependant adapter la méthode à chaque type de codage.

Ce type de démodulation a été utilisé lors de l'implémentation de la méthode sous Matlab mais n'est à ce jour pas implémenté en VHDL. Ce système a permis de mesurer les délais introduits par les relais et caractériser notre solution.

C. Démodulation par moyenne de niveau

Une autre solution permet de démoduler le signal sans retard introduit par le traitement du signal. Comme cela a été expliqué auparavant, un signal modulé en amplitude présente dans le cas des normes sans contact existantes deux amplitudes différentes. L'objectif de cette solution est de trouver dans un premier temps un seuil correspondant à l'écart d'amplitude entre le niveau haut et le niveau bas de la modulation d'amplitude puis de comparer le signal avec ce seuil. La figure III-22 montre de façon schématique les étapes de cette démodulation.

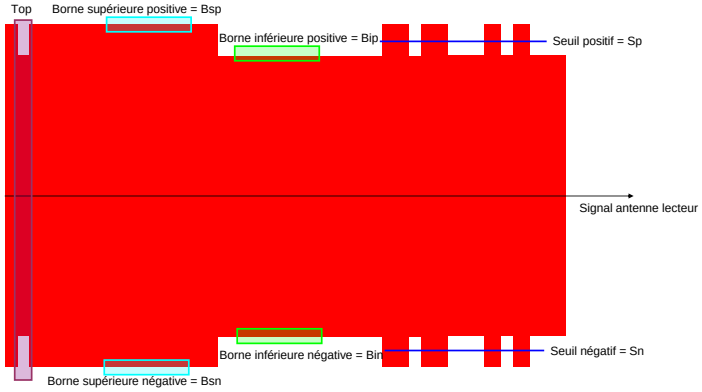


Figure III-22 – Démodulation par niveau signal

Dans un premier temps, le signal est non modulé (niveau haut d'amplitude), on calcule la moyenne des échantillons positifs et la moyenne des échantillons négatifs de façon à obtenir les valeurs Bsp et Bsn. De la même façon, le signal est modulé en amplitude (niveau bas d'amplitude) et on calcule la moyenne des échantillons positifs et négatifs de façon à obtenir Bip et Bin. On calcule à partir de ces valeurs les deux seuils, voir les équations III-6 et III-7.

$$S_p = B_{ip} + \frac{B_{sp} - B_{ip}}{2} \quad \text{(III-6)}$$

$$S_n = B_{in} + \frac{B_{sn} - B_{in}}{2} \quad \text{(III-7)}$$

On compare ensuite les échantillons du signal x avec ces deux seuils pour obtenir un signal binaire b, voir les équations III-8.

$$\begin{cases} si\ x(i) > 0\ et\ x(i) > S_p\ ou\ x(i) < 0\ et\ x(i) < S_n \Rightarrow b(i) = 1 \\ si\ x(i) > 0\ et\ x(i) < S_p\ ou\ x(i) < 0\ et\ x(i) > S_n \Rightarrow b(i) = 0 \end{cases} \quad \text{(III-8)}$$

C'est cette solution qui a été retenue pour l'implémentation sur FPGA dans le cadre de notre mesure de délai. Elle présente l'avantage d'être simple à mettre en œuvre et ne nécessite que peu de ressources. Aucun temps de traitement n'est nécessaire et surtout aucun filtrage qui pourrait modifier les temps d'établissement du signal.

PARTIE III. PREMIERES EXPERIMENTATIONS

1. Méthode de mesure

Avant l'implémentation de la contre-mesure sur FPGA, une campagne de mesures a été réalisée pour vérifier l'efficacité de la corrélation à mesurer des retards très faibles.

Notre banc de mesure (figure III-23) est composé de :

- Emission : Le dispositif d'émission choisi est le lecteur Lrfv7 (lecteur générique réalisé par le CEA Léti).
- Réception : Le module de réception est une carte RFID NXP Mifare Classic. Le module de réception n'a pas vraiment d'utilité puis les séquences envoyées n'ont aucune signification pour la carte. Cependant, cette carte permet de rabaisser l'amplitude de notre signal.
- Outils de mesure : Les bobines de calibration ont une sensibilité de 6 A/m/V. L'oscilloscope Lecroy Wavepro 735Zi employé lors des mesures permet d'échantillonner les signaux à 5GS/s.
- Relais : Relais filaire constitué d'un câble coaxial de 3m et deux antennes de fréquence centrale fc=13.56MHz, 50Ω Q=14

Lorsque la distance entre l'antenne lecteur et l'antenne du proxy augmente : l'amplitude du signal côté lecteur diminue et l'amplitude du côté carte augmente car l'influence de l'antenne du proxy diminue.

Un autre effet de l'augmentation de la distance antenne lecteur – antenne du proxy (antenne 1 du relais) est la diminution de l'amplitude de la sous-porteuse ce qui se traduit par une diminution du rapport signal sur bruit (SNR). Cette dernière rend le calcul de la corrélation plus complexe et surtout moins précis.

Une des variables des tests sera donc la distance entre l'antenne du proxy et l'antenne du lecteur dont les valeurs seront de 0, 5 ou 7 cm.

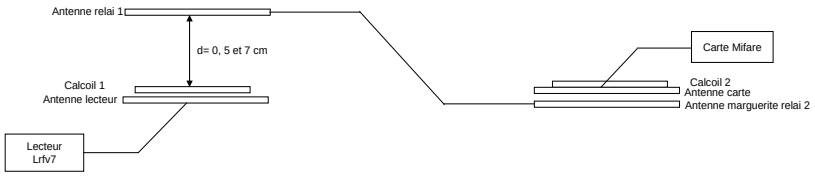


Figure III-23 – Mesures de délais pour plusieurs distances entre l'antenne lecteur et l'antenne 1 du relais

Lors de cette expérience, voir la figure III-23, la corrélation a été calculée dans plusieurs cas de figures mais toujours avec la même séquence de base. Les signaux sont dans un premier temps échantillonnés par la méthode d'échantillonnage implémentée sous Matlab (voir « Démodulation par position des extremums sur Matlab »).

2. Résultats de la corrélation

A. Corrélation classique

Ces courbes, voir les figures III-24 et III-25, montrent clairement que lorsque la distance entre l'antenne lecteur et l'antenne du proxy augmente, les pics de corrélation sont de plus faibles amplitudes. Il serait donc possible d'utiliser cette hauteur de pic pour déterminer la précision de notre mesure.

La distance entre deux pics de corrélation correspond à la période de notre signal, soit 1.18 µs.

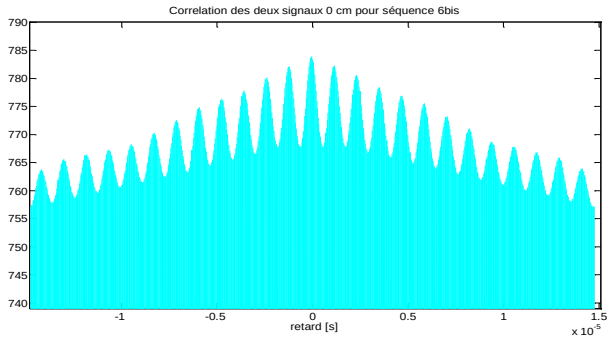


Figure III-24 – Corrélation à partir de signaux enregistrés sur l'oscilloscope pour les distances avec 0 cm entre les deux antennes.

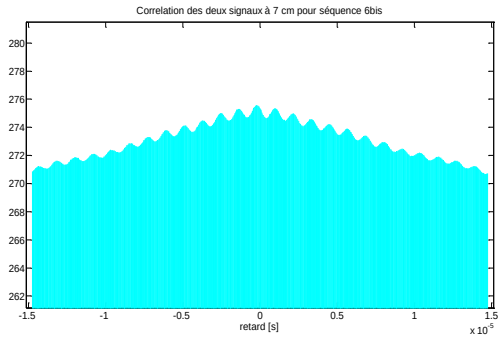


Figure III-25 – Corrélation à partir de signaux enregistrés sur l'oscilloscope avec 7 cm entre les deux antennes.

B. Corrélation par recherche d'extremum

On refait la même expérience en utilisant la méthode de la corrélation par recherche d'extremums. Les courbes (figures III-26 et III-27) montrent les résultats de cette corrélation

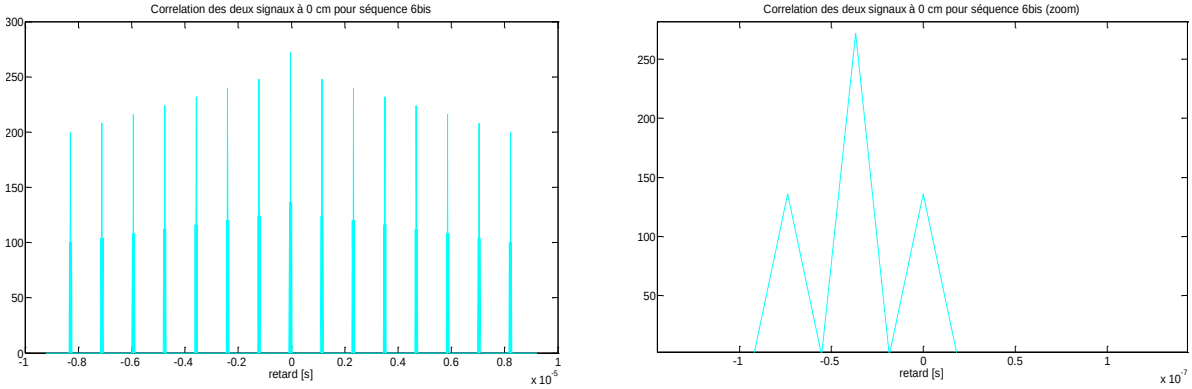


Figure III-26 – Corrélation de signaux enregistrés sur oscilloscope pour une distance de 0 cm entre le lecteur et l'antenne du proxy

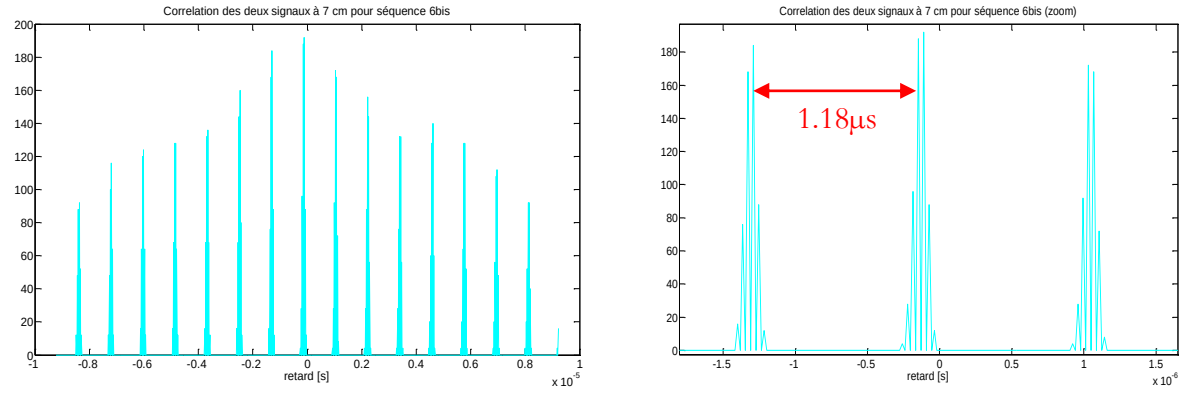


Figure III-27 – Corrélation sur des signaux enregistrés sur oscilloscope pour une distance de 7 cm entre le lecteur et l'antenne du proxy

Pour cette solution, la précision de notre mesure et sa validité peuvent être déduites de la largeur des pics. Plus la base du pic de corrélation est fine et plus la valeur trouvée est bonne. La largeur la plus fine que l'on puisse trouver est la période de la porteuse soit 73.75 ns. La largeur

du pic correspond aux décalages entre les extremums du signal utile trouvé lors de la recherche de maximum.

L'espace entre deux pics de corrélation correspond toujours à la période de notre signal soit 1.18 µs.

C. Résultats finaux

Le tableau III-2 montre les résultats de la corrélation pour les différentes distances entre l'antenne lecteur et l'antenne 1 du relais et pour les deux types de corrélation.

Tableau III-2 – Résultats de délais

	0 cm	5 cm	7 cm
Corrélation classique	Retard	Retard	Retard
essai 1	-73,75 ns	-221,24 ns	-221,24 ns
essai 2	-73,75 ns	-221,24 ns	-221,24 ns
essai 3	-73,75 ns	-221,24 ns	-221,24 ns
essai 4	-73,75 ns	-221,24 ns	-221,24 ns
Correlation par recherche d'extrémums			
essai 1	-36,87 ns	-221,24 ns	-184,37 ns
essai 2	-36,87 ns	-221,24 ns	-184,37 ns
essai 3	-36,87 ns	-221,24 ns	-184,37 ns
essai 4	-36,87 ns	-221,24 ns	-184,37 ns

Les résultats trouvés sont à peu près semblables pour les deux corrélations sachant que la deuxième méthode est beaucoup plus simple à implémenter car elle demande moins de ressources. Le retard dépend comme prévu de la distance entre les deux antennes.

PARTIE IV. LA SOLUTION

1. Présentation de la solution

L'objectif de notre solution est de détecter toutes les attaques de type relais quelque soit le délai introduit par ceux-ci. Notre solution détecte les attaques relais mais permet aussi d'authentifier la carte par le biais d'un protocole d'authentification basé à la fois sur des données cryptographiques et des informations de la couche physique de notre système. La détection de relais par la mesure ou le calcul du délai additionnel introduit par ce relais est une solution proche des protocoles appelés « distance bounding ». Nous avons déjà évoqué ce type de protocole dans la première partie consacrée à l'état de l'art. La solution est ici appliquée aux systèmes sans contact mais peut être utilisée pour d'autres types de communications sans fil.

Quelque soit le protocole de distance bounding utilisé, le lecteur envoie des requêtes auxquelles la carte répond. Entre la décision du lecteur, l'envoi de sa requête et la réception de la réponse de la carte, on trouve une multitude d'étapes de traitement du signal. Lorsqu'un relais est présent entre le lecteur et la carte, le nombre d'étapes est encore plus grand (figure III-28). Nous voulons identifier les délais additionnels introduits par le relais et donc les temps que nous pourrons mesurer avec notre système.

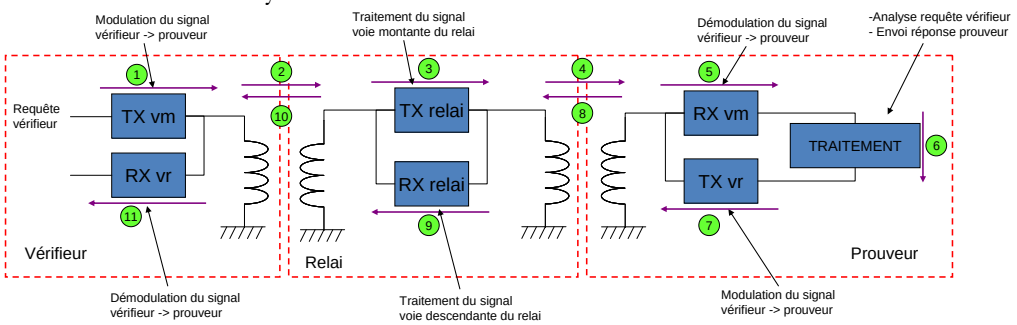


Figure III-28 – Temps de traitement des différentes étapes de la transmission d'une requête et de sa réponse

A chaque étape de traitement ou de propagation du signal correspond un certain temps de latence ; le tableau III-3 définit ces différents temps. On définit que les temps de propagation et les temps d'établissement dans toutes les antennes étaient identiques.

Tableau III-3 – Temps de traitement et de propagation du signal pour les différentes étapes

Etapes	Temps induit par l'étape	Symbole
1	Temps de modulation du signal par le vérifieur	t_{LTX}
2	Temps de propagation + Temps d'établissement dans les antennes	$t_P + 2t_E$
3	Temps de traitement de la voie montante du relais	t_{RTX}
4	Temps de propagation + Temps d'établissement dans les antennes	$t_P + 2t_E$
5	Temps de démodulation du signal par le vérifieur	t_{CRX}
6	Temps de traitement du prouveur pour calculer la réponse à envoyer	t_T
7	Temps de modulation du signal par le vérifieur	t_{CTX}
8	Temps de propagation + Temps d'établissement dans les antennes	$t_P + 2t_E$
9	Temps de traitement de la voie descendante du relais	t_{RRX}
10	Temps de propagation + Temps d'établissement dans les antennes	$t_P + 2t_E$
11	Temps de démodulation du signal par le vérifieur	t_{LRX}
Total	Délai mesuré entre la requête du vérifieur et la réception de la réponse du prouveur	t_D

Le temps qu'un système est susceptible de mesurer est le temps t_D, c'est-à-dire le temps entre l'émission de la requête et la réception de la réponse, voir équation III-9:

$$t_D = t_{LTX} + t_{LRX} + t_{CTX} + t_{CRX} + 4(t_P + 2t_E) + t_T + t_{RTX} + t_{RRX} \quad \text{(III-9)}$$

Ce temps t_D est composé d'un temps correspondant au système sans contact soit $t_{D1} = t_{LTX} + t_{LRX} + t_{CTX} + t_{CRX} + 2(t_P + 2t_E) + t_T$ et d'un temps spécifique au relais $t_{D2} = t_{RTX} + t_{RRX} + 2(t_P + 2t_E)$.Ces deux délais ne sont pas stationnaires, ils dépendent de la position des éléments entre eux, de la distance entre les antennes. On a donc $t_{D1} = t_{D1f} \pm \sigma$ et $t_{D2} = t_{D2f} \pm \delta$ avec t_{D1f} et t_{D2f} les parties déterminées du délai et σ et δ les parties variables.

L'objectif de notre contre-mesure est donc d'identifier dans un premier temps t_{D1f} et de trouver l'erreur admissible σ. Cette calibration permet de fixer une limite basse et une limite haute à la valeur de délais autorisés lors d'une authentification. Si le délai trouvé avec la solution est en dehors de cet intervalle, la solution conclut sur la présence d'un relais.

L'avantage de cette solution est que l'on ne mesure pas seulement un temps de propagation ; on mesure la différence de délai entre celui introduit par un système sans contact et celui introduit par un système sans contact en présence d'un relais.

2. Le protocole de sécurisation

La solution présentée utilise la fonction de corrélation pour calculer le retard introduit par le relais. Quel que soit le relais, le délai introduit par celui-ci peut être divisé en deux parties : la première partie est le délai introduit par la voie montante du relais (c'est-à-dire la partie du relais permettant de transmettre les informations du lecteur vers la carte) ; la deuxième partie est la voie

descendante du relais (c'est-à-dire la partie du relais qui transmet les informations de la carte vers le lecteur). Ces deux parties ont des valeurs de délais qui ne sont pas forcément identiques, notre solution mesure le délai total introduit par le relais sans pouvoir distinguer l'une des deux voies.

Le principe de base de la solution est le suivant ; la carte envoie un signal connu par le lecteur à un temps donné. Ce même signal auparavant généré par le lecteur peut alors être corrélé avec celui envoyé par la carte.

Notre protocole est proche d'un système de distance bounding ; il peut être divisé en trois phases : une phase d'initialisation, une phase consistant en un échange chronométré et une phase de vérification et conclusion (figure III-29).

La phase d'initialisation de notre protocole débute par l'envoi par le lecteur d'un nombre aléatoire à la carte. Le lecteur et la carte utilisent alors un algorithme cryptographique symétrique commun E_k avec k la clé secrète et le nombre aléatoire A échangé pour calculer T, le temps d'attente de la carte avant l'envoi de sa réponse ; et S, la séquence envoyée par la carte et synthétisée par le lecteur. Le calcul de T et de S à partir de la clé secrète permet d'authentifier la carte. Le lecteur n'est pas authentifié par la carte car l'objectif principal de notre solution est la détection de l'attaque relais. Cependant, de légères modifications de notre protocole peuvent permettre d'ajouter cette authentification mutuelle.

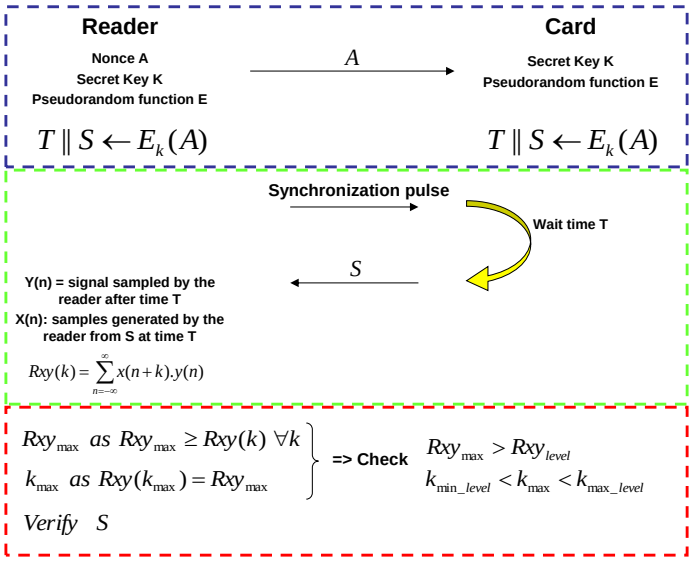


Figure III-29 – Protocole de notre système de détection

A la fin de l'émission de sa requête et cela après un temps aléatoire seulement connu du lecteur, celui-ci module brièvement son champ pour créer un top de synchronisation. Ce temps d'attente doit être inférieur au délai introduit par le relais pour éviter toute anticipation de cette impulsion par le relais. Cette impulsion est reçue par la carte avec un retard dépendant du temps Tr de propagation entre les antennes et du retard induit par le relais dans le cas où un relais est présent dans le champ RF. Il agit comme point de synchronisation du protocole pour le lecteur et la carte.

Une fois que ce top de synchronisation est reçu, la carte envoie la séquence S après le temps fixe T mesuré à partir du bit de synchronisation en en modulant sa charge. Le lecteur reçoit alors la séquence S', correspondant à la séquence S envoyée par la carte mais retardé par le lien inductif et la présence ou non d'un relais. Avant la réponse de la carte, le lecteur génère une séquence S en interne, générée au temps T. La séquence S' est synchronisée avec la séquence S par le biais du bit de synchronisation mais le retard introduit par le relais implique que les deux signaux sont décalés en temps. La séquence S générée est formée par les échantillons X(n) et la séquence S' par les échantillons Y(n).

La figure III-30 présente un synoptique de la solution proposée. Il est conçu sous une forme permettant l'identification des différentes phases de la solution. Trois axes apparaissent sur ce chronogramme, le premier est consacré aux signaux envoyés et reçus par le lecteur, le deuxième axe correspond aux signaux envoyés et reçus par la carte et le troisième axe aux données générées par le lecteur.

Pendant la phase de vérification, le lecteur corrèle les deux signaux S et S' de façon à déterminer le délai entre les deux séquences. L'index correspondant à la valeur maximum de la corrélation est le nombre d'échantillons correspondant au retard. Ce nombre d'échantillons est équivalent au délai introduit par le relais ; sa valeur permet de conclure sur la présence ou non d'un relais. De la même façon, le lecteur vérifie la séquence S reçue de façon à authentifier la carte. Lorsque le lecteur conclut qu'aucun relais n'est présent et que la carte est valide, il peut alors s'établir un échange de données confidentielles entre le lecteur et la carte.

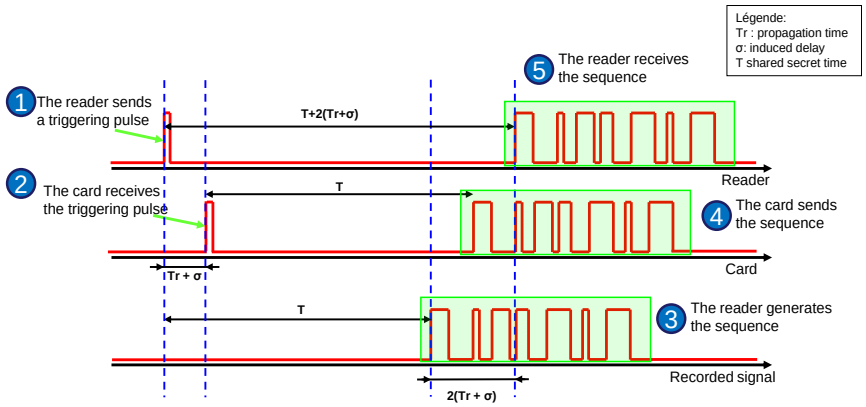


Figure III-30 – Solution proposée

3. Implémentation

Cette partie présente l'implémentation de la solution précédente au niveau du lecteur et de la carte. Les deux éléments possèdent chacun un composant en logique programmable ; il est ainsi possible de tester notre solution de façon totalement autonome. En effet, tous les tests précédemment réalisés nécessitaient des actions de notre part (enregistrement de signaux, traitement sous Matlab,…) ou du matériel en plus du système sans contact (oscilloscope, bobines de calibrations, …). L'implémentation d'un tel système directement sur carte permet de se rapprocher d'une solution finale pour la détection d'attaques relais.

Dans un système sans contact classique, le lecteur émet une requête et la carte envoie sa réponse après avoir interprété cette requête, voir la figure III-31. Entre la fin de l'émission du lecteur et le début de l'émission de la carte, les normes définissent un certain temps, appelé parfois temps de retournement, permettant à la carte d'interpréter la commande lecteur, de préparer sa réponse,…

Notre contre-mesure a pour objectif final de s'intégrer dans ce temps de retournement de façon à ne pas avoir à modifier les normes actuelles du sans-contact. Le circuit identifiant le top de synchronisation, générant la séquence et le temps aléatoire ainsi que le traitement de ces données devrait être dans un circuit indépendant du circuit interprétant les commandes du lecteur de façon à ne pas perturber le temps de retournement avant la réponse de la carte.

A l'heure actuelle, la contre-mesure remplace la réponse de la carte, la carte envoie la séquence aléatoire comme si cette séquence était la réponse de la carte à la requête du lecteur.

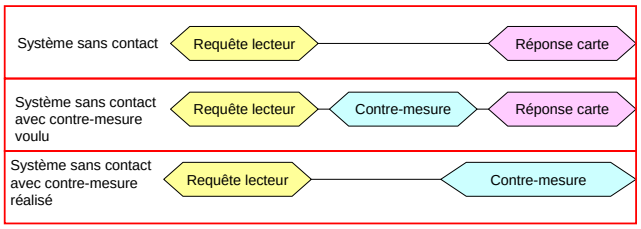


Figure III-31 – Placement de la contre-mesure dans le système sans contact

L'organigramme, voir la figure III-32, montre les différentes étapes et actions du lecteur et de la carte lors d'une séquence de recherche de présence de relais.

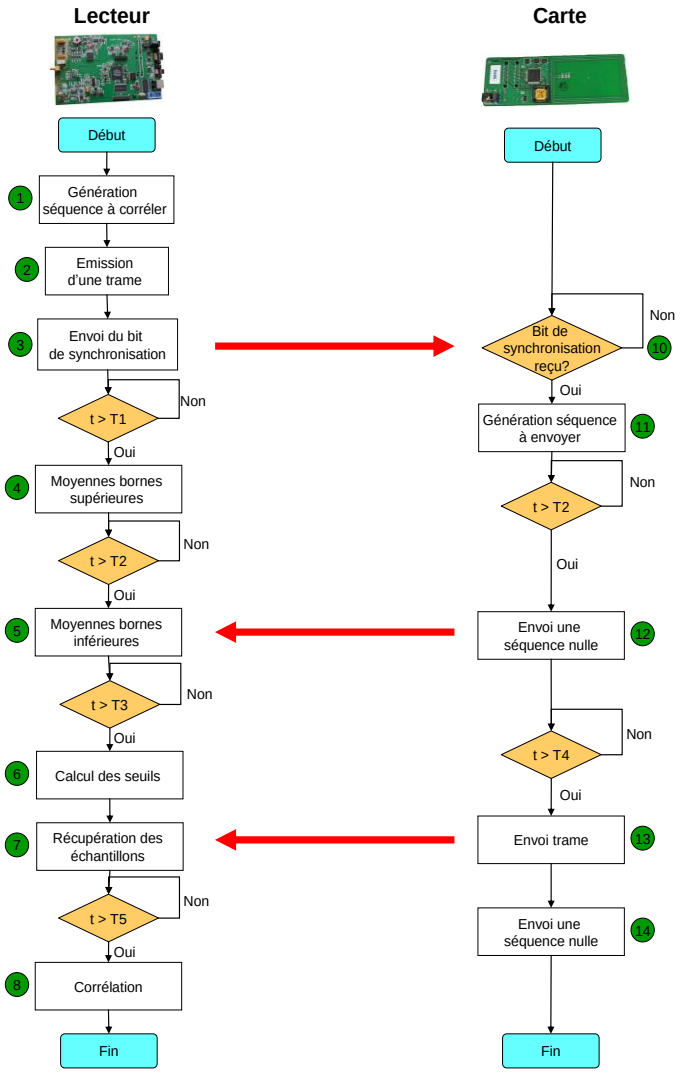


Figure III-32 – Organigramme des étapes de l'algorithme implémenté

Lors de cette implémentation, plusieurs données n'ont pas été prises en compte. Dans un premier temps, la séquence à corréler n'est pas envoyée pendant le temps de retournement de la carte. Cela nous laisse plus de temps pour envoyer la séquence voulue et faire les traitements nécessaires avant. Dans un deuxième temps, tout le protocole de cryptographie n'est pas appliqué ici, le lecteur et la carte génèrent chacun une séquence fixe donnée par l'utilisateur.

La figure III-33 permet de voir le rendu de ces différentes étapes sur le signal lui-même afin de mieux comprendre le fonctionnement du système.

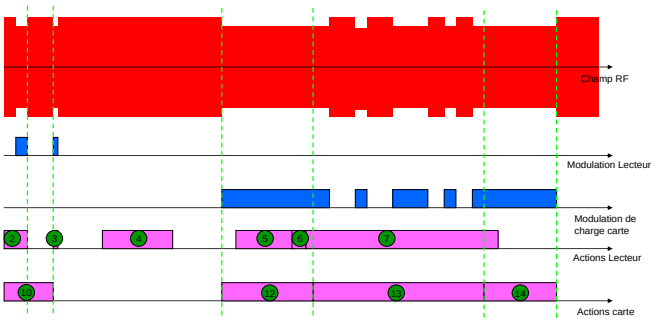


Figure III-33 – Chronogramme de la solution proposée

Chaque numéro sur les figures III-32 et III-33 représente une action à réaliser par le lecteur ou la carte. Chacune de ces actions est indispensable pour que la contremesure fonctionne :

Etape 1 : Cette étape consiste à générer côté lecteur la séquence qui sera corrélée avec celle reçue de la carte. Plusieurs données sont à prendre en compte : la fréquence d'échantillonnage du lecteur, le débit binaire de la carte, le nombre d'octets envoyés par la carte. Dans cette version de la solution, la carte envoie 4 octets soit 32 bits. Le débit binaire de la carte est de 424kbits/s et la fréquence d'échantillonnage du lecteur est de 27,12 MS/s. La séquence envoyée par la carte et reçue par le lecteur compte donc 2048 échantillons. La figure III-34 montre la conversion des octets à la conversion en échantillons par le lecteur.

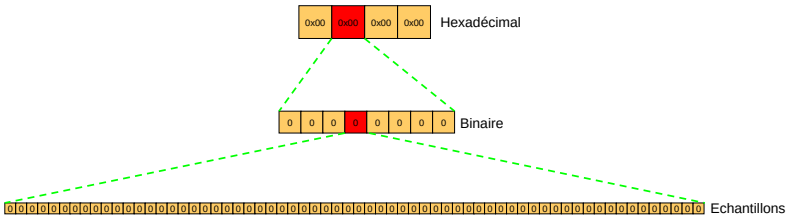


Figure III-34 – Génération de la séquence à corréler

De plus, il faut que le lecteur génère en plus de la séquence deux séries de '0' permettant le glissement d'un des signaux par rapport à l'autre lors de la corrélation. La séquence générée est la suivante, voir la figure III-35.

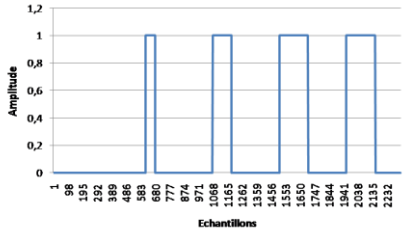


Figure III-35 – Séquence générée

Etape 2 : Cette étape concerne l'émission d'une trame par le lecteur. Dans cette version de la solution, le lecteur envoie un REQB selon la norme ISO14443-B en utilisant donc la modulation d'amplitude.

Etape 3 : Cette étape consiste à envoyer le top de synchronisation entre la carte et le lecteur à la fin de la transmission de la requête du lecteur. C'est donc le lecteur qui envoie ce top un temps aléatoire après l'EOF sous la forme d'une modulation de son champ RF.

Etape 4, 5 et 6 : Ces étapes sont abordées dans la section traitant de la démodulation par moyenne de niveau. L'étape 4 consiste à moyenner les valeurs échantillonnées par le lecteur de façon à obtenir les amplitudes moyennes positives et négatives du signal lorsque le champ n'est pas modulé. L'étape 5 procède de la même façon dans le cas où le champ est modulé, on trouve

donc des valeurs dont la valeur absolue est inférieure à celle trouvée lors de l'étape 4. L'étape 6 consiste à calculer les seuils de la manière décrite précédemment.

Etape 7 : L'étape 7 consiste à échantillonner le signal à la fréquence de 27,12MS/s. Chaque échantillon est comparé, selon s'il est positif ou négatif à la valeur d'un des seuils pour déterminer s'il correspond à un niveau logique '1' ou '0'.

Etape 8 : l'étape 8 est réalisée par un processeur NIOS intégré au composant FPGA, elle consiste à corréler le signal reçu avec celui généré par le lecteur et à déterminer le délai entre ces deux signaux. Selon la valeur du délai, le système peut alors conclure sur la présence ou on d'un relais.

Etape 10 : Cette première étape est une étape d'attente, la carte est en attente du top de synchronisation provenant du lecteur. La carte n'a aucune action à réaliser en attendant ce bit de démarrage.

Etape 11 : La carte génère de son côté la séquence à envoyer, cette séquence est pour le moment fixée par le développeur.

Etape 12 : Après un temps T2, ce temps correspondant à un temps nécessaire au lecteur pour réaliser l'étape 4, la carte envoie ensuite une séquence nulle. L'envoi d'une séquence nulle par la carte consiste en une modulation de sa charge; l'amplitude du signal est plus faible et le lecteur peut donc faire l'étape 5.

Etape 13 : La carte envoie ensuite la séquence à corréler.

Etape 14 : Cette étape consiste à renvoyer une nouvelle séquence de bits '0' de façon à permettre le glissement lors de la corrélation.

4. Problèmes rencontrés

Deux problèmes ont été identifiés lors de l'implémentation de cette solution dans le lecteur et la carte

A. Problème lié à l'alimentation

Lorsque la carte module le champ du lecteur pour permettre l'étape 5, la modulation de charge est assez longue. Or, l'alimentation de la carte dépend de l'amplitude de ce champ RF. Si le lecteur ou la carte module le champ trop longtemps, l'alimentation de la carte diminue avec une vitesse dépendant des capacités de découplage de la puce et peut réinitialiser la carte si l'alimentation diminue trop.

Comme on peut l'observer à la figure III-36, l'alimentation en jaune diminue lors de la réponse carte lors de la modulation de charge. Si la valeur de cette alimentation chute en dessous d'une certaine valeur de seuil, la carte se réinitialise. La durée de l'étape 12 et donc 5 prend en compte ce seuil.

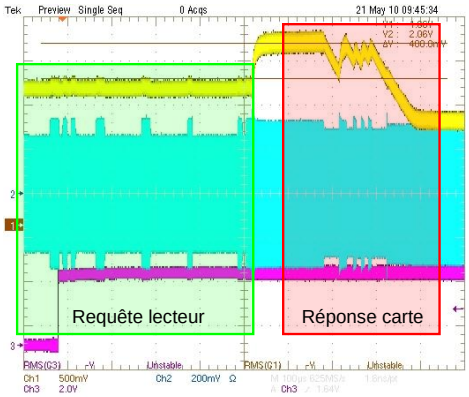


Figure III-36 – Courbe représentant l'alimentation de la carte en jaune et le champ RF en cyan

Toutes les cartes n'acceptent pas la même durée de modulation de charge, il faut donc faire attention que la carte ne se réinitialise pas. Il serait intéressant de comparer ce temps admissible par les différentes cartes sans contact des constructeurs actuels.

B. Inversion du signal

Selon la position de la carte, il est possible que, par le biais d'un couplage, le signal de la carte soit inversé. C'est à dire le niveau haut de champ est au niveau bas et inversement. Il est nécessaire de traiter cette éventualité en ajustant les conditions sur la valeur binaire '1' ou '0' du signal.

5. Expérimentations

L'implémentation de la solution sur un lecteur et une carte sans contact conforme aux standards ISO14443, voir la figure III-37 nous permet de tester les relais que nous avons développés dans la section Réalisation d'attaques.

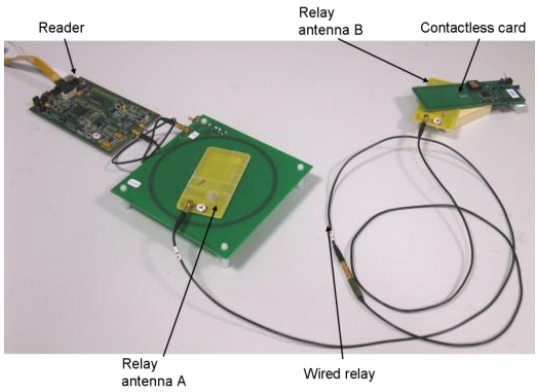


Figure III-37 – Expérimentations sur un relais filaire

Nous exécutons notre protocole en présence des trois relais réalisés et aussi sur le système sans contact sans relais. Une routine est réalisée de façon à obtenir 500 valeurs de retards pour chaque scénario avec des distances entre les éléments de 0 à 6 cm.

A partir de ces valeurs de retard, il est possible de réaliser un histogramme par scénario comme nous pouvons l'observer sur la figure III-38.

Le diagramme montre un histogramme distinct dans chaque cas : les 3 relais et le cas sans relais. L'histogramme représentant le système sans relais est en partie à cheval avec le relais filaire car la différence de délais occasionnés par ces deux systèmes est plus faible que la précision de notre système de détection.

La précision actuelle ne permet pas de détecter toutes les attaques relais filaires. Le dernier pic correspondant à l'histogramme du relais filaire correspond aux délais occasionnés par le système sans contact lorsque la carte est à 6 cm de notre lecteur. En réduisant la distance d'activation de notre lecteur, il est donc possible d'augmenter le pourcentage de relais détectés par notre système.

Les figures III-39 et III-40 présentent les différents délais trouvés pour deux scénarios, le relais filaire et le système sans contact sans relais. Dans le cas du scénario sans relais, on retrouve ce qui avait été dit précédemment, c'est-à-dire que pour une distance de 6 cm entre le lecteur et la carte, l'histogramme est excentré par rapport aux autres.

Dans le cas du relais filaire, les histogrammes sont assez proches les uns des autres mais l'on remarque que plus la distance augmente et plus le pic maximal de l'histogramme correspond à un délai de plus en plus important ce qui montre que la distance a bien une influence sur le délai introduit par le relais. Comme l'attaquant ne peut pas rapprocher la carte du relais, les délais introduits par le relais seront assez longs pour être détectés.

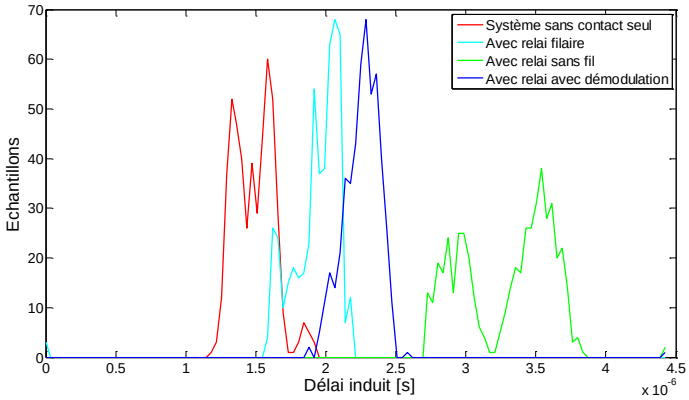


Figure III-38 – Délais obtenus pour tous les scénarios

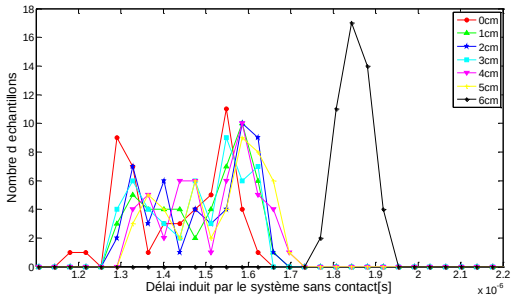


Figure III-39 – Délais obtenus pour le scénario sans relais en fonction de la distance entre le lecteur et la carte

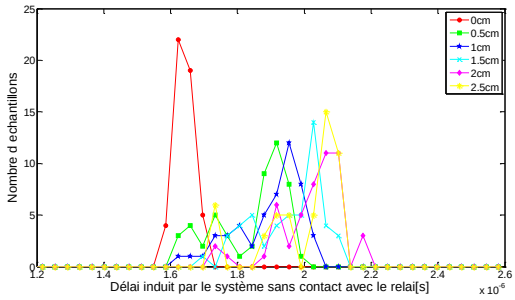


Figure III-40 – Délais obtenus pour le scénario relais filaire en fonction de la distance entre l'antenne 2 du relais et la carte

PARTIE V. ANALYSE DU PROTOCOLE

1. Comparaison avec les recommandations de Hancke [HAN2010]

Pour se protéger des différentes attaques possibles au niveau de la couche physique, le design d'un protocole de distance bounding doit suivre quelques recommandations. Notre protocole n'est pas un protocole de distance bounding mais il est intéressant de noter les différences entre les principes de notre système et ceux recommandés dans la littérature :

- Utiliser un canal de communication avec une vitesse de propagation proche de celle de la lumière dans le vide : la propagation des ondes électromagnétiques est proche de la vitesse de la lumière. Notre système est en accord avec ce principe.
- Ne pas utiliser un format de trames particulier ; cela inclut les en-têtes, les délimiteurs, les corrections d'erreur bit de parité, …. Notre système est en accord avec ce principe.
- Minimiser la taille d'un symbole utilisé pour représenter un bit. Notre système est en accord avec ce principe puisque chaque bit est codé en NRZ.

L'utilisation d'un canal de communication permettant de diminuer la durée d'un bit permet bien d'améliorer la précision du système. Pour respecter la norme sans contact et ne pas ajouter d'électronique supplémentaire, nous avons conservé la fréquence porteuse de notre système.

- Contraintes matérielles :
  - Le vérifieur dispose de plus de ressources que le « prouveur », c'est donc lui qui calcule la corrélation des signaux et qui gère le protocole.

- Contrairement à leur recommandation, la réponse du « prouveur » est générée de manière synchrone avec l'horloge du « verifieur » Cela peut être la base d'attaques temporelles comme celles décrites par Hancke dans l'article [HAN2008-B].

- Synchronisation : Pour échanger des données, le « vérifieur » et le « prouveur » ont besoin d'une référence temporelle. L'impulsion de synchronisation utilisée par notre système répond à ces exigences.
- Résolution temporelle : Il n'est pas possible d'améliorer cette précision puisque le canal de communication utilisé n'offre pas une résolution très importante. On a cependant pu observer que cette précision suffisait à authentifier la majorité des relais.

2. Sécurité

Le principal objectif de notre système était de montrer qu'il est possible de développer des solutions permettant de détecter des relais sans modifier des standards sans contact (utilisation de la même fréquence porteuse). Le protocole d'authentification et de sécurisation n'est pas parfait au sens cryptographique du terme. La multitude de solutions cryptographiques existantes dans ce domaine n'impose pas de recherche supplémentaire. Nous nous sommes donc consacrés à la couche physique de notre protocole et avons étudié sa résistance aux attaques temporelles en particulier.

A. Attaques au niveau de la couche physique

a. Résistance au bruit

L'utilisation de systèmes radiofréquences à bande large comme la modulation UWB est sensible au bruit en raison de la faible densité de puissance spectrale sur toute la largeur du spectre. Cette faiblesse des communications à large spectre avantage l'attaquant puisque des erreurs de bits peuvent apparaître en raison d'un canal bruité. Lors d'un protocole de distance bounding, le « vérifieur » peut confondre des erreurs de bits introduites par un canal bruité et des erreurs sur des bits anticipés par le relais et faux dans un canal non bruité. Ainsi, le « vérifieur » peut penser que la carte sans contact est proche de lui et il ne parvient pas à détecter le relais.

Cette attaque est seulement possible dans des systèmes à large bande et notre système n'est pas sensible à ces erreurs. D'une part, le canal sans contact est moins sensible au bruit et la réponse de la carte aux requêtes du lecteur est une trame constituée de plusieurs bits

b. Attaques basées sur l'accélération du temps d'horloge

La fréquence de l'horloge permettant à la carte sans contact d'opérer correspond à la fréquence de la porteuse générée par le lecteur. La norme impose que cette fréquence soit égale à 13.56 MHz avec une tolérance de 7 kHz (0.05%de la fréquence porteuse). En pratique, une carte sans contact ne possède pas les ressources permettant de vérifier qu'un lecteur est conforme avec cette norme. Un lecteur peut donc augmenter la valeur de cette fréquence de façon à accélérer le rythme des opérations effectuées par la carte sans contact. Cette attaque décrite par G. Hancke ajoute une importante faille pour les protocoles de distance bounding [HAN2008-B]. En effet, un attaquant peut accélérer l'horloge de la carte de façon à obtenir sa réponse plus vite, diminuer le délai introduit par le relais et ainsi prouver que la carte est dans la zone de fonctionnement du lecteur. Dans cet article, l'auteur parvient à obtenir une réponse de la carte alors que la fréquence de la porteuse est de 15.56 MHz.

Cependant, l'article [REI2007] nous permet d'affirmer que certaines solutions permettent de limiter l'accélération de cette horloge, en particulier l'utilisation de filtres passe-bas détectant certains niveaux de hautes fréquences ou l'utilisation d'horloge interne à la carte. Ces solutions peuvent permettre de limiter l'accélération de l'horloge à quelques % de la fréquence porteuse. Un attaquant peut absorber de 2 à 3 ns par cycle d'horloge.

Nous allons tenter de déterminer la longueur de la séquence S et la durée du temps T maximum pour que l'accélération de l'horloge n'ait pas d'impact sur notre système.

Pour cela, il est nécessaire d'étudier deux points :

- Le traitement nécessaire par le relais pour accélérer la fréquence de la porteuse
- L'accélération des temps de traitement par le relais

Un dispositif relais permettant d'accélérer la porteuse du signal émis par le lecteur doit démoduler le signal de façon à modifier la fréquence de la porteuse. La seule phase que le relais peut accélérer est le temps secret T de notre protocole, correspondant à l'attente entre l'impulsion de synchronisation et le début de la réponse carte. La carte mesure ce temps en comptant un certain nombre de coups d'horloge. Si cette horloge est plus rapide, ce temps diminue et le la réponse carte est émise plus tôt. L'objectif du relais est de compenser le retard introduit par sa chaîne de traitement.

Dans la partie « Réalisation d'attaques », nous avons développé un système relais permettant la démodulation du signal lecteur. Le délai introduit par la chaîne de démodulation et modulation de la voie montante est de 600 ns. Le délai introduit par le traitement de la voie descendante est proche de 1.4 µs. On suppose que les délais introduits entre le lecteur et le proxy, le môle et la carte sont proches de 0 pour faciliter la compréhension du système. La figure III-41 montre les différentes phases de transmission du relais et celle que le relais peut accélérer.

Le relais doit donc compenser un délai de 2 µs en diminuant de 3 ns le temps de chaque cycle d'horloge. Pour supprimer un tel retard, il serait nécessaire que le temps secret soit supérieur à environ 600 périodes d'horloge, soit 44 µs. Pour se prémunir d'une telle attaque, il est donc nécessaire que la valeur du temps secret T soit inférieure à 44 µs.

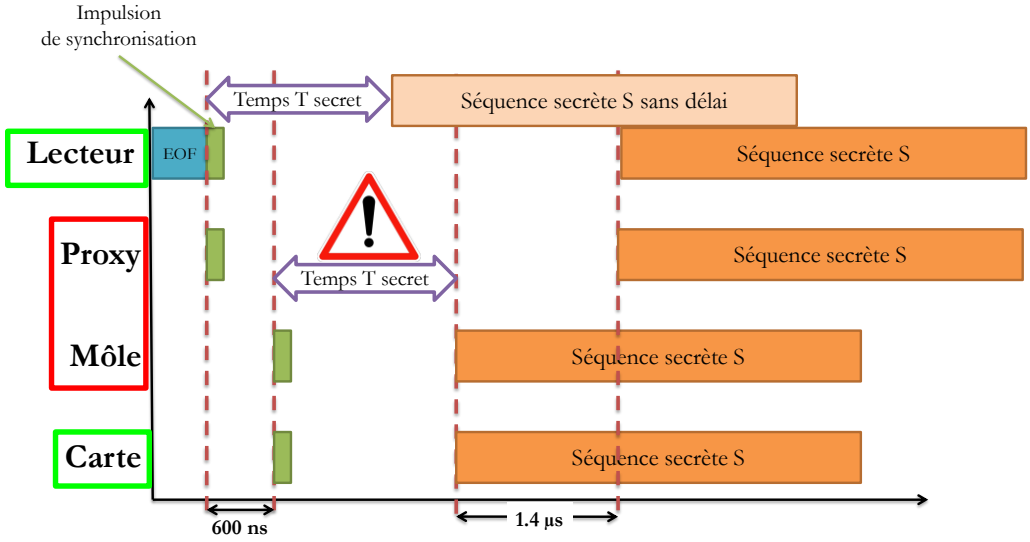


Figure III-41 – Attaque basée sur l'« overclocking »

c. Anticipation du bit de synchronisation par l'attaquant

Dans notre protocole, le bit de synchronisation ne contient pas de challenge et le relais n'a pas besoin d'attendre son émission par le lecteur pour le transmettre à la carte sans contact. Il lui est possible d'anticiper et d'envoyer ce bit à la carte à la fin de la requête lecteur. Il peut ainsi compenser le traitement de la voie montante du relais voir figure III-42.

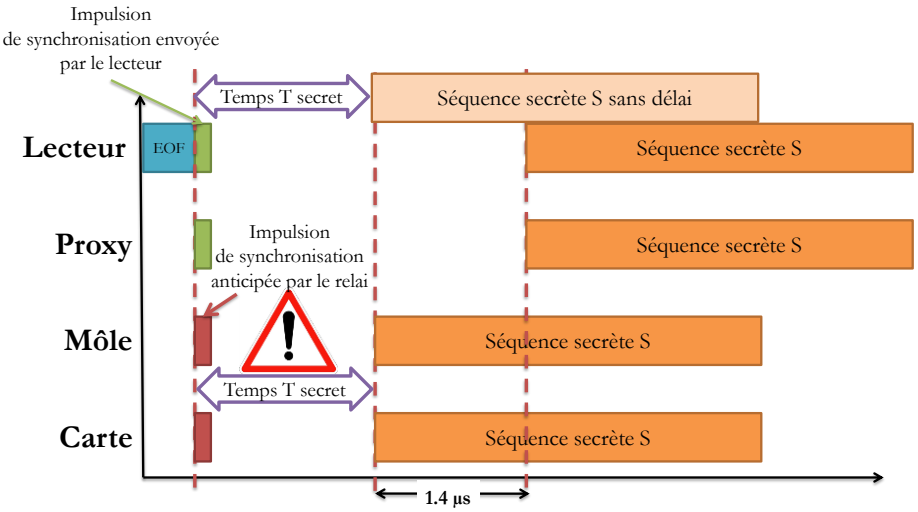


Figure III-42 – Attaque basée sur l'anticipation du bit de synchronisation

Cependant, l'anticipation de ce bit de synchronisation n'est pas suffisante lorsque ce dernier est envoyé à la fin de la requête par le lecteur. En effet, la voie de traitement descendante du relais ne sera pas compensée.

Une autre solution consiste à ajouter un challenge dans ce bit de synchronisation en développant une modulation à plusieurs niveaux. Selon le niveau d'amplitude (ou de phase) du ce bit, la carte attend un temps T ou T' et envoie une séquence S ou S'. Le front-end RF permettant d'utiliser une modulation à plusieurs niveaux a déjà été développé au sein du CEA Léti dans le cadre d'une extension de la norme sans contact vers le très haut débit. Cette solution permet aussi d'envoyer le bit de synchronisation à la carte après un temps aléatoire suivant la fin de la requête et uniquement connu du lecteur.

B. Sécurité cryptographique

a. Authentification

Les attaques de type « rejeu » (replay) ou clonage sont détectées puisque la carte sans contact est authentifiée par le lecteur. En effet, la carte doit connaître la clé secrète et l'algorithme de cryptage pour calculer le temps T et la séquence S. Si l'authentification mutuelle du lecteur et de la carte est nécessaire, il est possible de modifier la phase d'échange de nombres aléatoires de façon à vérifier que le lecteur connait la clé secrète.

b. Amélioration de la sécurité

Pendant une même transaction entre le lecteur et la carte, il est possible d'améliorer la sécurité en répétant plusieurs fois notre protocole de manière aléatoire entre les différentes trames échangées entre le lecteur et la carte. Dans ce cas, la séquence S et le temps T doivent être recalculés en reprenant le même algorithme cryptographique soit $T^n||S^n \leftarrow E_k^n(A)$ pour empêcher une attaque de type « replay ». Ainsi, il n'est pas nécessaire pour le lecteur de renvoyer un nouveau challenge A.

C. Autres attaques

Généralement, la plupart des protocoles de distance bounding sont confrontés à trois attaques de façon à analyser leur sécurité. Nous avons exposé notre système aux mêmes attaques.

a. L'attaque « Distance fraud »

L'attaque « distance fraud », voir la figure III-43, est une attaque impliquant seulement un lecteur et une carte sans contact. Le lecteur n'est pas acteur de cette fraude, seule la carte sans contact réalise l'attaque. Bien que les deux dispositifs soient trop éloignés pour une communication standard, la carte doit convaincre le lecteur qu'elle est près de lui.

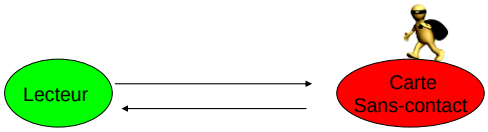


Figure III-43 – Attaque « Distance Fraud »

b. L'attaque « Terrorist fraud »

Cette attaque, voir la figure III-44, implique une carte, un lecteur sans contact et un relais permettant une communication entre le lecteur et la carte. Le lecteur et la carte ne sont ni auteurs de la fraude, ni conscients de cette fraude ; seul le relais réalise la fraude. Le relais doit convaincre le lecteur que la carte est à proximité de lui.

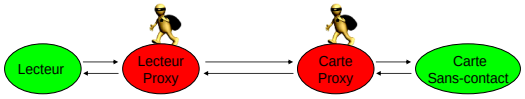


Figure III-44 – Attaque "mafia fraud"

c. L'attaque « Mafia fraud »

Cette attaque, voir la figure III-45, est très proche de l'attaque précédente, la seule différence est que la carte sans-contact et le relais collaborent pour tromper le lecteur sur la distance qui les sépare.

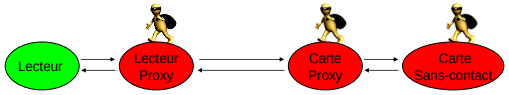


Figure III-45 – Attaque «terrorist fraud »

L'étude de cette attaque au niveau de la couche physique montre que la carte détenue par l'attaquant doit être capable de communiquer avec un lecteur à une distance supérieure à celle de fonctionnement standard.

Si l'on se réfère à l'article [SIN2007], certaines règles permettent de vérifier qu'un protocole de distance bounding est sécurisé contre ces trois attaques :

- Il est important de vérifier que la carte (le « prouveur ») connait la clé secrète k.
- Pour prévenir les attaques « mafia fraud », notre protocole consiste en une série d'échanges très rapides. En calculant le délai introduit par ces différents échanges, le lecteur peut détecter la présence d'un relais. Pour éviter que la carte ne réponde trop tôt, chaque challenge est aléatoire et imprévisible ; la réponse dépend de ce challenge.
- Pour prévenir les attaques « terrorist fraud », il est nécessaire que la phase d'authentification de la carte (le « prouveur ») et la phase d'échanges rapides soient liées par un algorithme cryptographique.

Nous pensons que notre protocole est conforme à toutes ces règles de design. Seule l'attaque distance fraud nécessite l'utilisation obligatoire d'un bit de synchronisation basé sur une modulation multi-niveaux.

Les attaques de type « rejeu » (replay) ou clonage sont détectées puisque la carte sans contact est authentifiée par le lecteur. En effet, la carte doit connaître la clé secrète et l'algorithme de cryptage pour calculer le temps T et la séquence S.

PARTIE VI. AMELIORATIONS A PREVOIR

1. M-séquences

Les M-séquences présentent des propriétés permettant d'améliorer la précision et la génération de séquences de notre solution. Ces M-séquences sont des séquences pseudo-aléatoires employées dans de nombreuses applications cryptographiques. Deux propriétés des M-séquences sont particulièrement intéressantes : l'aspect aléatoire et ses propriétés de corrélation. La séquence se compose d'impulsions dont la largeur est variable et proportionnelle à la durée de la période minimale.

A. Définition

La figure III-46 montre la constitution d'une M-séquence. Cette séquence est constituée d'impulsions de largeur variable mais multiple de T. Pour une durée de séquence NT et si elle se répète indéfiniment, sa fonction d'autocorrélation, représentée sur la figure III-47 est constituée de triangles de largeur à base 2T se répétant tous les NT.

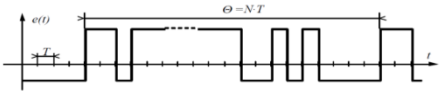


Figure III-46 – définition d'une M-séquence

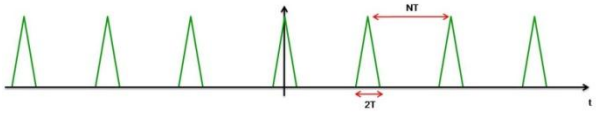


Figure III-47 – Autocorrélation d'une M-séquence se répétant indéfiniment

B. Implémentation d'une M-séquence

Les générateurs LFSR produisent ce qu'on appelle des « linear recursive sequences » (LRS). La durée de la séquence et sa répétition dépendent de l'état initial et des contre-réactions utilisés. Elles permettent de générer ce qu'on appelle des M-séquences.

Il existe deux types d'implémentations des générateurs LFSR :

- L'implémentation selon Fibonacci, voir la figure III-48, est composée de registres à bascule et d'additionneurs binaires modulo 2 (C'est-à-dire que 0+0=0, 0+1=1, 1+1=0). Les résultats de ces additions correspondent à la donnée d'entrée.

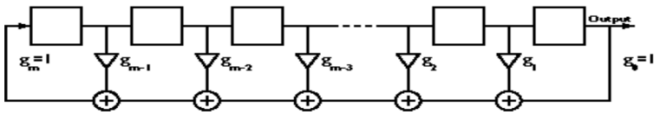


Figure III-48 – Implémentation Fibonacci

Sur ce schéma, les g_i ont pour signification '1' pour connexion et '0' pour pas de connexion (circuit ouvert). Cependant, g_0 et g_m sont des exceptions puisqu'ils sont toujours à 1.

- L'implémentation selon Gallois, voir la figure III-49(appelé aussi MRSRG = Modular Shift Register Generator), consiste en plusieurs registres à bascule comme pour Fibonacci, cependant chaque sortie de bascule est additionnée à l'état futur selon la valeur de g_i.

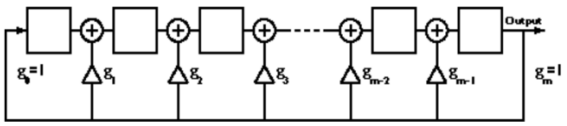


Figure III-49 – Implémentation Gallois

Ces deux implémentations produisent la même séquence mais les états initiaux seront différents pour obtenir la même séquence.

C. Propriétés des M-séquences

- Un LFSR de m bits génère des séquences de périodes 2^m-1 bits
- Une M-séquence contient exactement 2^{m-1} '1' logiques et 2^{m-1}-1 '0' logiques
- Si une M-séquence est étudiée comme un signal analogique et temporel, en établissant que chaque '0' binaire vaut -1 et chaque '1' binaire vaut 1, alors la fonction d'autocorrélation sera de valeur 1 pour un délai nul et -1/ (2^m-1) pour tout autre délai supérieur à 1 bit que ce délai soit positif ou négatif. La forme de cette fonction d'autocorrélation entre -1 et 1 bit est triangulaire et centrée sur 0. De ce fait, la fonction va croître linéairement du temps -1 jusqu'au temps 0 et décroître du temps 0 au temps +1. En clair, l'autocorrélation d'une M-séquence est très proche d'une approximation de la fonction delta de Kronecker

Le tableau III-4 présente pour un nombre de bascules données du LFSR, les caractéristiques de la M-séquence générée.

Tableau III-4 – Récapitulatif des caractéristiques des M-séquences en fonction de leur nombre de bascules

nombre de bascules (n)	longueur de la séquence maximale (2^n-1)	nombre de séquences maximales	exemple d'un polynôme pour n donné	écriture octale de ce polynôme
2	3	1	$1+x+x^2$	7
3	7	2	$1+x+x^3$	13
4	15	2	$1+x+x^4$	23
5	31	6		45
6	63	6	$1+x+x^6$	103
7	127	18		211
8	255	16		435
9	511	48	$1+x^4+x^9$	1021
10	1023	60	$1+x^3+x^{10}$	2011
11	2047	176	$1+x^2+x^{11}$	4005
12	4095	144	$1+x+x^4+x^6+x^{12}$	10123
13	8191	630	$1+x+x^3+x^4+x^{13}$	20033
14	16383	756	$1+x+x^6+x^{10}+x^{14}$	42103
15	32767	1800	$1+x+x^{15}$	100003

Comme on peut le voir dans le tableau, un polynôme possédant un nombre de séquences maximales important, correspond à une longueur de séquence importante. Par exemple pour le polynôme d'ordre 15, le nombre de séquences différentes réalisables avec ce polynôme est de 1800 mais la longueur de la séquence est alors de 32767 périodes d'horloge.

D. Comparaison avec d'autres codages

Pour vérifier qu'une M-séquence présente un réel avantage par rapport à une suite classique pseudo-aléatoire, nous avons implémenté à l'aide de bascules D un LFSR. Ce LFSR, composé de 6 bascules permet donc de générer des M-séquences de longueur 63 bits. La figure III-50 présente l'implémentation d'un tel LFSR :

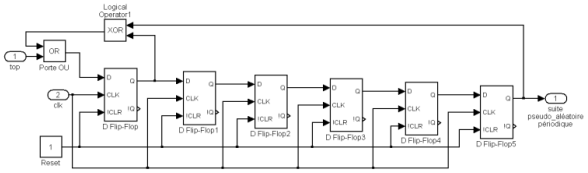


Figure III-50 – Implémentation d'un LFSR sous Simulink

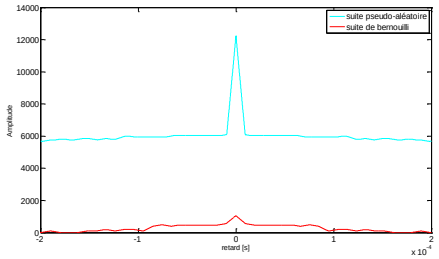


Figure III-51 – Comparaison de l'autocorrélation d'une M-séquence et d'une suite Bernoulli

Nous avons ensuite comparé la fonction d'autocorrélation de cette M-séquence avec la fonction d'autocorrélation de séquences dites de Bernoulli. Le résultat, voir la figure III-51, montre une différence significative entre les deux courbes. Le pic de corrélation obtenu avec une M-séquence par rapport à celui obtenu avec un générateur de Bernoulli est beaucoup plus important et précis.

2. Délai introduit par le top

Une amélioration importante concerne la détection du top de synchronisation qui sert de point de référence entre le lecteur et la carte. Le manque de précision de notre solution est en grande partie dû à l'identification de l'impulsion du lecteur par la carte. Sur la version actuelle de notre solution, la carte comporte une puce permettant de démoduler le signal du lecteur, le signal de sortie de cette puce est le signal que nous pouvons traiter avec de la logique programmable. Le retard induit par la démodulation de ce top a été mesuré dans différentes conditions : avec et sans relais, et pour plusieurs distances entre les éléments. Les résultats, voir la figure III-52, montrent que le délai est constitué d'un retard fixe dépendant de la chaîne de traitement et d'autres paramètres et d'un retard variable dépendant en partie du couplage entre les antennes. La détection du bit de synchronisation est très peu précise et induit une faible précision de notre système de détection.

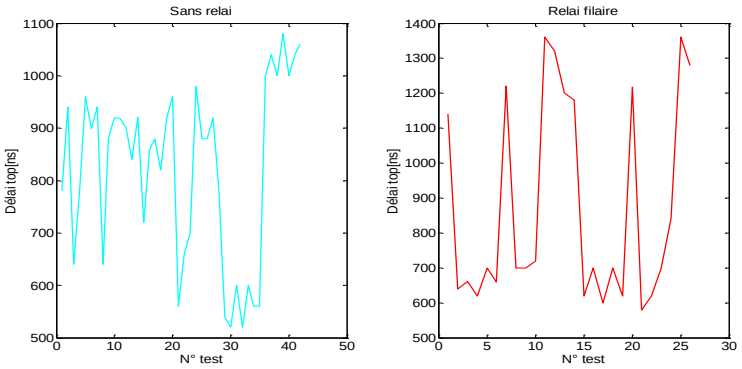


Figure III-52 – Précision de la réception du top de synchronisation dans le cas avec et sans relais

Notre système devra être capable de détecter le top de synchronisation en un temps fixe. Ce temps ne doit pas ou peu nuire à la précision de notre système. Il peut être de quelques périodes de porteuse mais il doit être précis et d'une durée indépendante de la distance entre les antennes.

3. Modulation de phase

A l'heure actuelle, Le Japon et les Etats-Unis ont déjà mis en place l'utilisation des technologies NFC pour le paiement. Ces technologies, dans le cadre d'une communication active, permettent aux deux dispositifs de générer leur propre champ RF. Le destinataire de la communication peut répondre en modulant son champ RF en phase. Nous pensons en effet que la modulation de phase peut permettre d'améliorer la précision de notre système de détection. Nous avons observé auparavant que la modulation d'amplitude, de part le temps d'établissement de la sous-porteuse et de l'amplitude de ses pics réduisait de façon significative la précision de notre système.

A. Définition

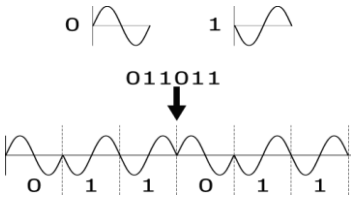


Figure III-53 – La modulation de phase: chaque état binaire correspond à un changement de phase du signal

La modulation de phase est une modulation permettant de transmettre un signal en modifiant la phase de la porteuse, voir la figure III-53.

B. Données sur la précision d'un système utilisant une telle modulation

Un changement de phase, de même qu'un changement d'amplitude lors d'une modulation n'est pas immédiat. Un certain temps est nécessaire avant que le changement d'état soit effectif. Cependant, le changement d'état est plus rapide dans le cas de la modulation de phase même si le temps d'établissement de cette phase dépend en grande partie du changement de phase à réaliser lors d'une transition.

Plus l'excursion de phase est faible et plus le temps d'établissement du changement de phase est rapide car cela ne demande pas de fréquence trop élevée.

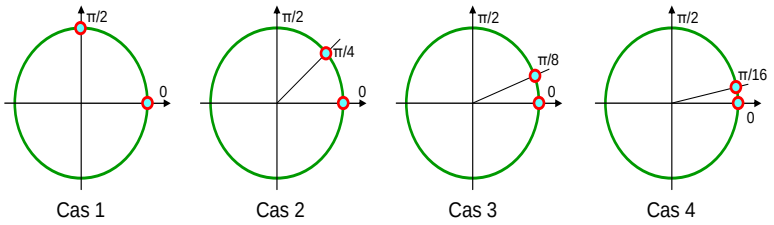


Figure III-54 – Plusieurs excursions de phase

La figure III-54 montre plusieurs possibilités lors d'une transition d'état. Plus l'excursion est faible et plus il sera difficile à observer, mais plus le changement d'état sera rapide et n'influera pas sur l'amplitude.

La figure III-55 montre la modulation de phase pour une excursion de phase allant de $\pi/2$ pour un même signal binaire de départ.

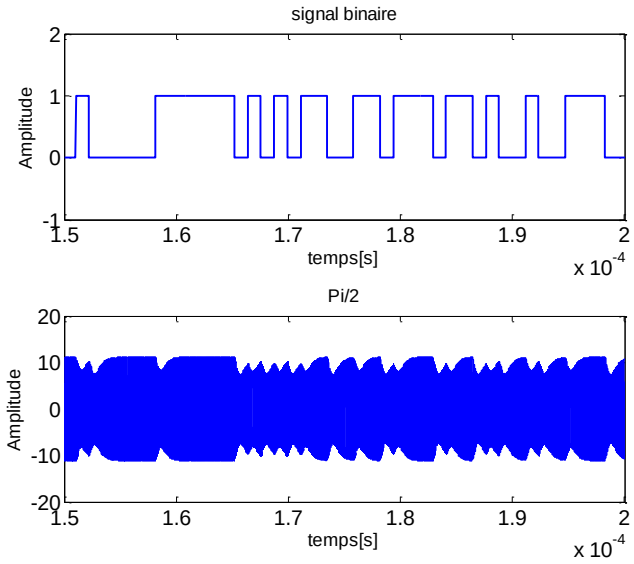


Figure III-55 – Modulation de phase pour différentes excursions de phase

La figure III-56 montre le spectre de signaux modulés en phase. On remarque que plus l'excursion de phase est grande et plus la modulation de phase apporte des fréquences élevées.

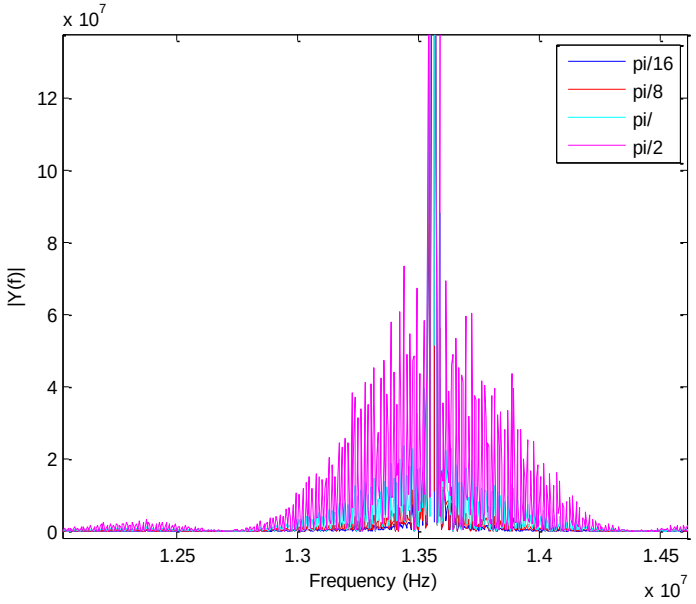


Figure III-56 – FFT d'un signal modulé en phase dans le cas de plusieurs excursions de fréquence

Ces fréquences élevées sont filtrées par le système sans contact dont la bande passante est proche de 13.56 MHz, ce qui apporte un temps d'établissement de la phase plus ou moins grand. Il faut donc faire un compromis entre le temps d'établissement et l'observabilité de l'excursion de fréquence par notre système.

La figure III-57 montre le même signal, mais après passage par une fonction de transfert correspondant à un système sans contact. Lorsque l'excursion en fréquence est trop importante, on observe une modulation d'amplitude en plus de la modulation de phase.

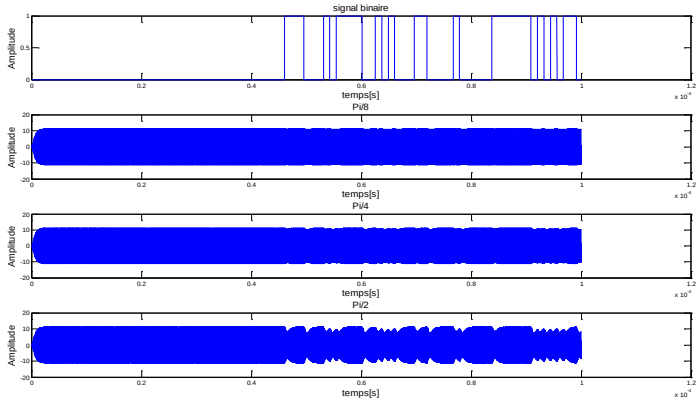


Figure III-57 – Modulation de phase d'un système sans contact selon l'excursion de phase

Pour conclure sur la modulation de phase, ce type de modulation ne peut pas être utilisé pour tous les systèmes sans contact pour le moment, mais plus sur les systèmes NFC qui génèrent leur propre champ RF. Dans le cas d'un système où la sécurité doit être importante, l'utilisation d'un dispositif actif peut être intéressante. Ceci peut nous permettre d'utiliser la modulation de phase qui semble présenter plus d'avantages que la modulation d'amplitude.

4. Amélioration réalisée

Les relais filaires (2 antennes et un câble coaxial) sont des attaques particulièrement difficiles à détecter par un dispositif. Malgré leur manque de transparence, la rapidité de ces systèmes complique la mise en place de contre-mesures adaptées. Les délais introduits par ces relais avoisinent les 300 ns, comme nous avons pu le mesurer auparavant. Nous avons montré que le manque de précision de notre système était en grande partie dû à la démodulation du top de synchronisation envoyé par le lecteur. La modulation d'amplitude ne permet pas d'avoir une résolution temporelle suffisante pour détecter de tels délais.

Disposant d'une carte sans contact permettant de démoduler des signaux modulés en phase (figure III-58), l'objectif est d'observer si la modification de notre point de référence peut permettre d'améliorer la précision de notre système. Cette carte sans contact d'expérimentation a été développée au CEA-Léti ; elle est utilisée pour le THD (très haut débit) et possède un front-end RF démodulant les signaux en phase. Une caractéristique importante de cette carte est qu'elle est passive ; elle ne possède aucune source d'énergie autre que le champ RF du lecteur.

Pour ne pas complexifier notre système, nous avons décidé de moduler en phase uniquement le top de synchronisation. Le protocole a été implémenté sur le lecteur et la carte sans contact en intégrant les différentes modifications. La principale difficulté que nous avons rencontrée a été de garder un système téléalimenté en présence du relais. En effet, la puissance récupérée au niveau de la carte sans contact est faible et permet uniquement une téléalimentation lorsque la carte est proche du lecteur. La présence du relais introduit une diminution du champ radiofréquence et de la puissance reçue au niveau de la carte, le relais filaire ne fonctionne que pour certaines distances entre le relais et la carte sans contact.

Cependant, il est intéressant de voir si le relais est détecté pour les distances de fonctionnement de la carte. La figure III-59 présente deux histogrammes correspondant aux distributions de délais dans le cas avec et sans relais filaire. On observe que ces deux histogrammes sont très différents, la présence du relais introduit un délai supplémentaire que notre système n'a aucun mal à détecter. La largeur de la base de notre histogramme permet d'avoir une idée de la précision de notre détecteur de relais ; on trouve une valeur avoisinant les 200 ns. Cette valeur est plus de deux fois plus faible que celle trouvée pour un système utilisant un top de synchronisation modulé en phase.

Cette expérience démontre que toutes les attaques de relais peuvent être détectées. Cependant, cette amélioration peut impliquer la modification des front-end RF sur les cartes sans contact actuelles.

Figure III-58 – Carte sans contact d'expérimentation avec un front end F démodulant la phase

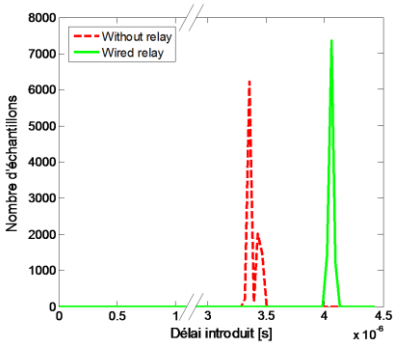


Figure III-59 – Résultats obtenus avec l'amélioration de la précision du top de synchronisation

Le délai introduit n'est plus le même pour les mêmes attaques car le front-end de la carte et le traitement du signal ne sont pas les mêmes.

Conclusion du chapitre

L'attaque relais est l'attaque la plus dangereuse basée sur la couche physique des systèmes sans contact. Cette attaque doit être sérieusement prise en compte car elle est simple à implémenter et qu'elle peut être utilisée dans de nombreuses applications. De plus, l'utilisation croissante de cette technologie et l'arrivée de la NFC dans les téléphones portables donnent l'accès à de nouvelles opportunités pour les hackers. Les lecteurs sans contact actuels ne permettent pas de détecter tous les types de relais. Ces attaques ne modifient pas le signal, ne perturbent pas la communication et introduisent de très faibles délais dans la communication. De plus, les protocoles cryptographiques ne permettent pas de détecter cette attaque.

Nous avons développé une nouvelle solution permettant de mesurer des délais très faibles. Cette contre-mesure utilise la méthode de corrélation pour calculer le retard introduit par le relais. Ce retard est alors utilisé pour conclure sur la présence d'un relais entre le lecteur et la carte. Pour la première fois, une solution permettant la détection de relais a été développée et implémentée sur un système sans contact. Cette solution n'exige aucune modification hardware du lecteur et de la carte. Elle permet de mesurer des retards très faibles, de l'ordre de 300 ns. Cette solution est parfaitement compatible avec les normes sans contact actuelles et elle ne perturbe pas les transactions entre le lecteur et la carte. Seul le relais le plus critique, le relais filaire, n'est pas détecté dans quelques rares cas. Nous avons développé une nouvelle solution qui détecte tous les types de relais en améliorant la précision de notre chaîne de mesure. Cependant, cette méthode nécessite la modification du front end RF de la carte sans contact.

Chapitre IV. Utilisation du canal sans-contact

Introduction du chapitre

L'utilisation du canal de communication pour sécuriser un système ou des transactions est une méthode privilégiée. En effet, un des principaux avantages d'une telle solution est la difficulté à décrypter une telle sécurité pour un attaquant. Un canal de communication présente généralement des caractéristiques propres au couple émetteur-récepteur et au support de l'information. Ces spécificités sont difficiles, voire impossibles à copier par un pirate. Celui-ci ne dispose pas des moyens et des informations permettant de découvrir et d'analyser toutes les caractéristiques utilisées par la contre-mesure. Les PUFs (Physically Unclonable Function) sont un autre exemple de contremesures difficiles à copier par un attaquant.

Deux solutions, utilisant la couche physique des systèmes sans contact et permettant d'obtenir une empreinte physique du système utilisé, ont été développées. Ce chapitre est donc divisé en deux sous-parties traitant chacune d'une des solutions apportées.

La première contre-mesure développée est basée sur la modification de la réponse à un échelon ou à une impulsion en présence d'un autre système à boucles inductives. L'antenne d'un lecteur possède une fonction de transfert évoluant en fonction du couplage avec d'autres systèmes inductifs. La mesure et l'analyse des réponses obtenues au niveau du lecteur peut permettre d'authentifier une carte ou de détecter la présence d'un relais.

La seconde contre-mesure a pour objectif d'utiliser le bruit pour détecter la présence d'un relais de type « amplify and forward ». Entre un émetteur et un récepteur, un tel relais amplifie le signal utile, mais aussi le bruit au niveau de l'émetteur et du récepteur. Il est alors possible de mesurer ce bruit et de déduire de ses différentes caractéristiques la présence d'un relais.

PARTIE I. SOLUTION BASEE SUR LA REPONSE IMPULSIONNELLE DES SYSTEMES SANS CONTACT

Dans cette partie, nous avons développé les bases d'une contre-mesure pour les attaques de la couche physique basée sur l'analyse de la réponse impulsionnelle. Les antennes des circuits du lecteur et de la carte sans contact peuvent être modélisées par de simples circuits R, L, C. Cette nouvelle contre-mesure utilise les principes de ce type de circuits oscillants pour déterminer certains paramètres au niveau du lecteur sans contact. Ces différents éléments permettent de détecter la présence d'une carte à proximité du lecteur, de mesurer le couplage entre une carte et un lecteur et de détecter la présence de certains relais de type « amplify and forward ». Cette solution consomme très peu d'énergie, ne demande aucune modification hardware au niveau du front end RF de la carte et fonctionne avec la plupart des cartes sans contact existantes.

Dans un premier temps, nous détaillerons le fonctionnement de notre solution et ses différents modes de fonctionnement. Une large étude basée sur des simulations des systèmes sans contact a été réalisée.

Dans un second temps, nous présenterons les premières expérimentations qui ont été réalisées, et comparerons ces premiers résultats à la théorie.

1. Principe de base

Sans activer le champ radiofréquence du lecteur, il est possible d'utiliser les caractéristiques de la couche physique des systèmes sans contact pour identifier certains paramètres de notre système. Pour la plupart des systèmes sans contact utilisant le couplage inductif pour transmettre puissance et données, l'antenne du lecteur peut être modélisée par un circuit électrique oscillant consistant en une résistance, une inductance et une capacité mises en série. Le comportement temporel d'un tel circuit lorsqu'un signal impulsionnel ou un échelon est appliqué en entrée est appelé le régime d'oscillations libres amorties. Le courant dans le circuit varie sous la forme d'une exponentielle décroissante modulée à la fréquence de résonance du circuit RLC. D'une part, une

carte sans contact peut aussi être modélisée par un circuit RLC parallèle résonant approximativement à la même fréquence que celle du lecteur. D'autre part, lorsque la distance entre le lecteur et la carte est faible, il se crée un couplage entre les deux circuits. On peut donc penser que la carte a une influence sur la fonction de transfert du système global et sur la réponse temporelle à une impulsion ou un échelon. L'analyse de la réponse à un échelon ou à une impulsion peut permettre de mesurer l'influence de n'importe quel système (carte, relais,…) à proximité d'un lecteur. La figure IV-1 décrit le modèle électrique d'un système sans contact ; c'est-à-dire un lecteur et une carte liés par un couplage k.

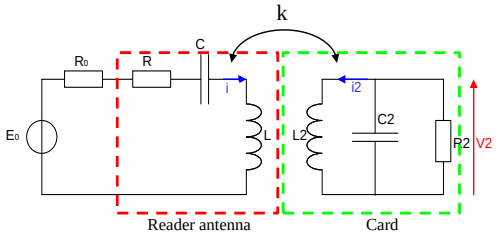


Figure IV-1 – Modèle électrique d'un système sans contact

A partir des équations électriques d'un système sans contact simple, un modèle a été développé au sein du CEA sous la forme d'une S-fonction simulable sous Simulink. Ce modèle nous permet de visualiser le courant dans l'antenne du lecteur lorsqu'une impulsion ou un échelon est injecté en entrée. Dans la suite de cette étude, le signal utilisé en entrée de l'antenne lecteur sera un échelon car nous avons observé qu'une impulsion (au sens d'une impulsion de Dirac) n'apportait pas assez d'énergie à notre système pour observer un courant assez important dans l'antenne lecteur.

Lorsque le couplage entre l'antenne du lecteur et celle de la carte est nul, la carte est éloignée du lecteur et n'a aucune influence sur son antenne. Dans ce cas, le modèle électrique est simplement le circuit associé à l'antenne lecteur, c'est-à-dire un circuit R, L, C série. Comme on l'a précisé précédemment, la forme d'une telle réponse sont des oscillations amorties. Dans le cas d'un couplage nul, le courant obtenu dans l'antenne du lecteur est décrit sur la figure IV-2.

Selon la littérature, le couplage entre l'antenne du lecteur et celle de la carte est compris entre 3% et 20% lorsque les deux dispositifs sont dans la même zone de communication. [PAR2003]. La figure IV-3 décrit le comportement du courant dans l'antenne du lecteur lorsqu'il y a un couplage assez fort entre les deux antennes, c'est-à-dire lors de la présence d'une carte.

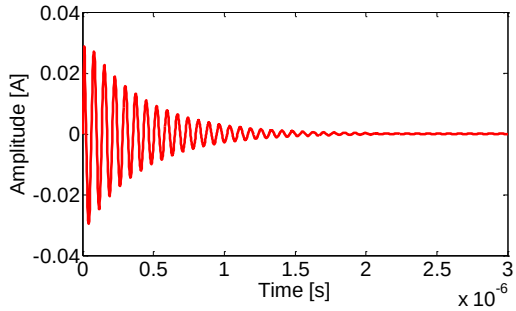


Figure IV-2 – Réponse à un échelon sans présence d'une carte sans-contact

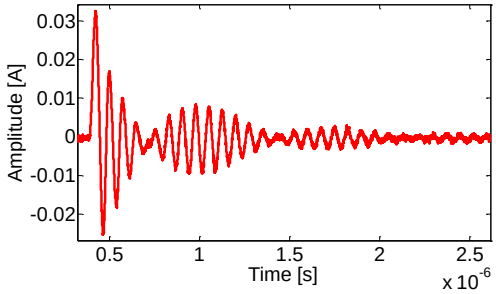


Figure IV-3 – Réponse à un échelon en présence d'une carte sans-contact, k=10%

Les deux réponses observées sur les figures IV-2 et IV-3 ont des comportements très différents. Le couplage entre deux circuits électriques résonants a bien une influence sur la forme du courant dans l'antenne du lecteur. Pour les deux systèmes, on observe une oscillation à la même fréquence correspondant à la fréquence de résonance du circuit. Cependant, alors qu'on observe bien une exponentielle décroissante pour la réponse dans le cas sans carte, on observe

des « rebonds » dans le cas avec carte. Le courant dans l'antenne du lecteur varie donc en fonction du système global, il est donc possible de déterminer certaines caractéristiques sur notre système en connaissant la réponse de notre lecteur avec et sans carte.

Comme on l'a vu précédemment, la réponse temporelle d'un circuit R, L, C à un échelon se traduit par une variation exponentielle de la tension au niveau du lecteur. Basée sur [PAR2003], l'expression mathématique de ces variations se présente sous la forme de l'équation IV-1.

$$v(t) = V_{max} e^{-t/\theta} \cos(\omega t) \quad \text{(IV-1)}$$

avec $e^{-t/\theta}$ la décroissance logarithmique dépendant de θ, la constante de temps de notre système donnée par l'équation IV-2.

$$\theta = \frac{2L}{R} \quad \text{(IV-2)}$$

Le coefficient de qualité de l'antenne est défini par l'équation IV-3 dans le cas d'un circuit R, L, C série.

$$Q = \frac{Lw}{R} \quad \text{(IV-3)}$$

On obtient alors l'équation IV-4.

$$\theta = \frac{Qf_0}{\pi} = \frac{Q}{\pi} T_0 \quad \text{(IV-4)}$$

avec f_0 et T_0 respectivement la fréquence, soit 13.56MHz, et la période des oscillations soit 73.74 ns. La figure IV-4 montre les caractéristiques temporelles de la réponse impulsionnelle.

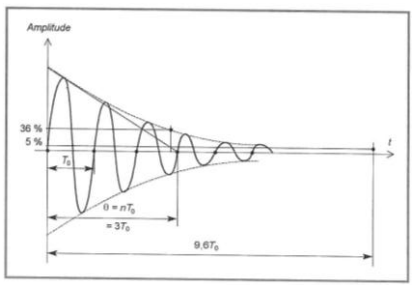


Figure IV-4 – Réponse impulsionnelle et caractéristiques temporelles [PAR2003]

Au bout d'un temps T= 3θ, la tension aux bornes de la résistance est égale à 5 % de la tension Vmax ; l'énergie disponible dans le condensateur s'est alors très fortement dissipée.

Le coefficient de qualité est donc un facteur très important, en particulier la résistance R. En effet, plus cette résistance est faible et plus le condensateur se charge vite en énergie. On observe aussi que la durée de la réponse impulsionnelle augmente lorsque le coefficient de qualité augmente.

2. Simulations

A. Méthode d'analyse

Il est intéressant de connaître les caractéristiques du signal à envoyer permettant d'obtenir une réponse simple à analyser. Les deux paramètres importants sont le temps de montée de l'échelon et sa durée.

a. Etude du temps de montée de l'échelon

On fixe une durée d'échelon infinie et on fait varier le temps de montée entre 1 ps et 1 µs. Pour vérifier que c'est bien le temps de montée et non la rapidité de cette montée qui a un impact sur la réponse indicielle, on réalise la même expérience pour un échelon de 5 V (figure IV-5) et

un échelon de 2 00V (figure IV-6).

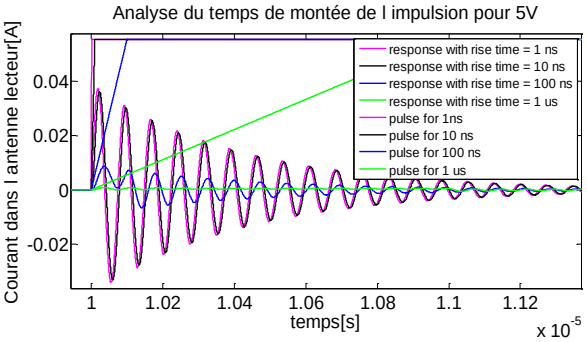


Figure IV-5 – Analyse du temps de montée pour une impulsion de 5 V

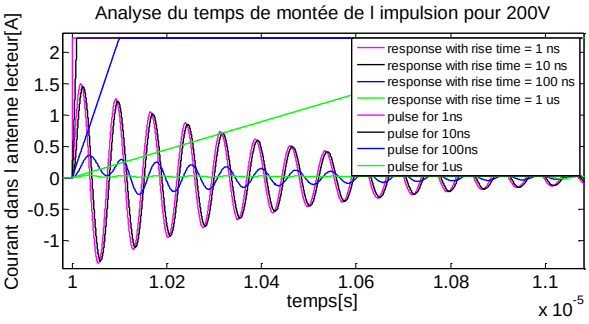


Figure IV-6 – Analyse du temps de montée pour une impulsion de 200 V

En conclusion, le temps de montée est très important. Il doit être supérieur au temps de montée d'une sinusoïde de fréquence 13.56 MHz. Sa limite basse n'est pas importante mais cette durée doit être inférieure à 10 ns pour avoir des oscillations d'amplitude optimale.

b. <u>Etude de la durée de l'échelon</u>

On fixe un temps de montée à 1 ps et on fait varier la durée de l'échelon entre 0 et 100 ns, voir la figure IV-7.

Plus intéressant que d'avoir un échelon très long, on peut modifier le signal d'entrée de façon à obtenir un signal carré et des transitoires périodiquement. Ainsi, on peut injecter un échelon toutes les 4 us, puisque l'on a deux réponses par impulsion: une sur le front montant et une sur le front descendant. Le plus important n'est pas la durée de l'échelon mais le temps de montée et de descente de celui-ci.

La durée minimum de l'échelon est donc de 10 ns. En dessous de cette valeur, la réponse obtenue aura une amplitude trop faible ou sera distordue.

Pour comprendre ce phénomène, on s'intéresse à la FFT des différents échelons (figure IV-8).

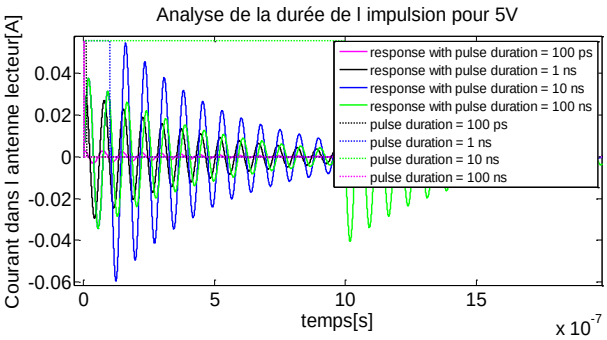


Figure IV-7 – Analyse de la durée de l'impulsion

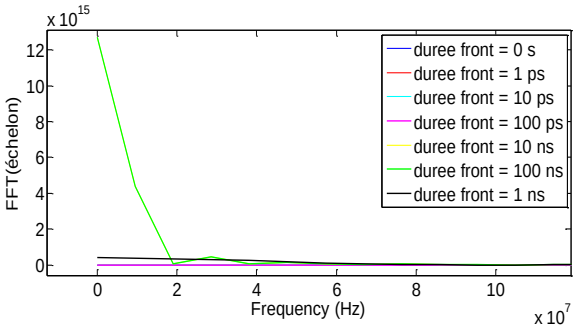


Figure IV-8 – FFT des impulsions en fonction des durées de l'impulsion

On remarque rapidement que l'énergie est distribuée différemment selon la durée de l'échelon. Plus l'échelon est rapide et plus le spectre est large. Si la gamme de fréquences s'élargit, l'énergie se répartit sur plus de fréquences différentes. C'est pour cette raison que le condensateur peut stocker suffisamment d'énergie pour obtenir une réponse claire uniquement si l'échelon a une largeur temporelle assez importante, c'est-à-dire supérieure à 10 ns.

B. Couplage et détection de carte

Il est possible de simuler, à l'aide de notre modèle, le couplage entre un lecteur et une carte, mais aussi de faire varier sa valeur. Le couplage permet d'obtenir une indication sur la proximité de la carte par rapport au lecteur. La réponse à un échelon nous permet à la fois de savoir si le lecteur détecte une carte sans contact dans sa zone de communication, mais aussi de connaître une valeur approchée du couplage entre les deux antennes. En effet, la figure IV-9 montre des réponses différentes selon la valeur du couplage. Alors que la réponse impulsionnelle est une simple oscillation amortie de manière exponentielle, on observe un ou plusieurs rebonds. Plus le couplage est important et plus le nombre de rebonds est important et plus le premier rebond est proche du début de la réponse.

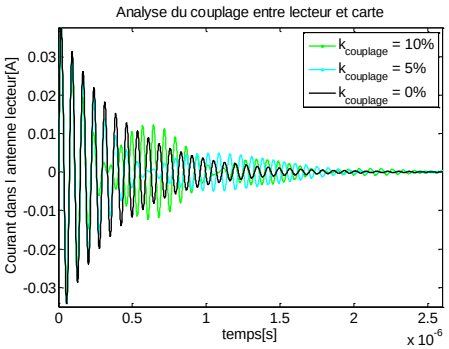


Figure IV-9 – Analyse des réponses en fonction du couplage

a. Influence de la bande passante de l'antenne lecteur

Comme on peut l'observer sur les figures IV-10 et IV-11, plus la bande passante de l'antenne lecteur est sélective et plus la décroissance du signal dans l'antenne est lente. Cette caractéristique est importante car elle permet d'obtenir un temps d'observation plus long. Les résultats obtenus sont en concordance avec la théorie où l'on voit que la décroissance est fonction du facteur de qualité. Plus celui-ci est grand et plus la décroissance est longue. Plus la résistance du lecteur est faible et plus le courant traversant l'antenne est important. Ainsi, le condensateur se charge plus rapidement et à la fin de la phase de transition de l'échelon, le condensateur contient plus d'énergie.

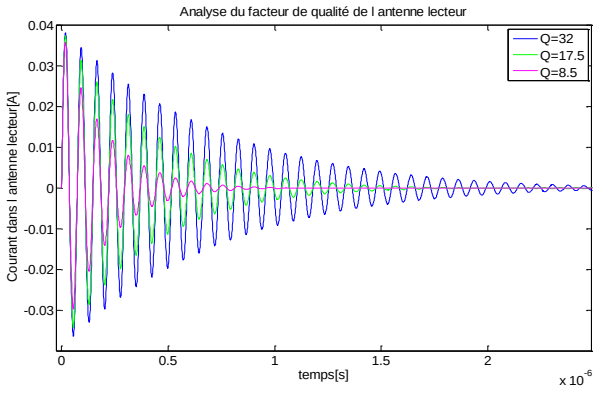


Figure IV-10 – Analyse du facteur de qualité de l'antenne lecteur (couplage nul)

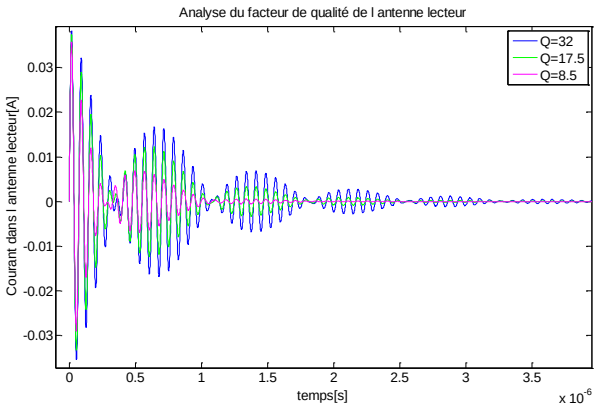


Figure IV-11 – Analyse du facteur de qualité de l'antenne lecteur (couplage 10%)

La décharge du condensateur est donc plus longue avec un courant de décharge plus important. Ce paramètre est donc très intéressant puisqu'il va nous permettre d'analyser une réponse de plus forte amplitude et l'observation des oscillations sur un temps plus important.

b. Influence de la bande passante de l'antenne carte

De la même façon, la bande passante et donc le facteur de qualité de l'antenne de la carte sans contact ont une influence intéressante sur la réponse à un échelon. Même si cette différence est moins marquée que pour la variation du facteur de qualité de l'antenne lecteur, on observe sur la figure IV-12 que plus le facteur de qualité de l'antenne carte est élevé et plus l'amplitude des oscillations est importante. L'explication est la même que précédemment, la résistance étant plus faible, la quantité d'énergie que le condensateur décharge est plus élevée. Le coefficient de qualité a une influence sur l'amplitude, mais aussi légèrement sur le déphasage lors des différents rebonds. En général, les cartes ont des coefficients de qualité assez élevés et il est difficile de les discerner pour de fortes valeurs. Cependant, un système assez précis peut être capable de déterminer le coefficient de qualité de l'antenne carte. Dans le cas d'un système parfait, on pourrait être capable de discerner différentes cartes simplement par leurs coefficients de qualité différents.

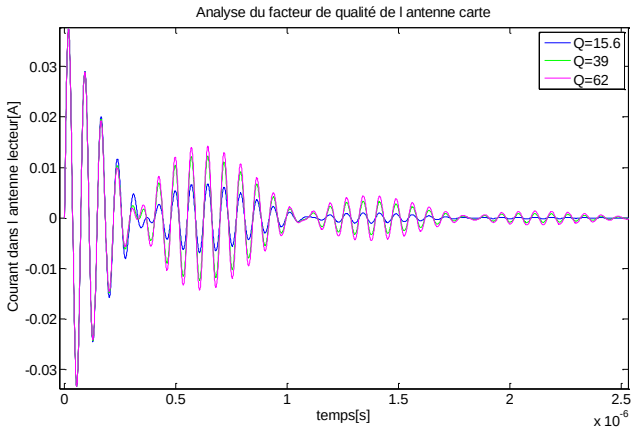


Figure IV-12 – Analyse du facteur de qualité de l'antenne carte (couplage 10%)

C. Détection de relais

Puisque la réponse à un échelon permet de caractériser un système sans contact, il est possible qu'on puisse différencier cette réponse lorsque le lecteur est près d'une carte sans contact dont il connait la courbe caractéristique ou lorsqu'il est près d'un relais de type 'amplify and foward'. Ce type de relais a été introduit et implémenté dans le chapitre consacré à la réalisation d'attaques. Ce sont des relais qui ne démodulent pas le signal et qui se comportent en simples transmetteurs d'informations. Le relais filaire a été modélisé sous Matlab et simulé sous Simulink, voir la figure IV-13.

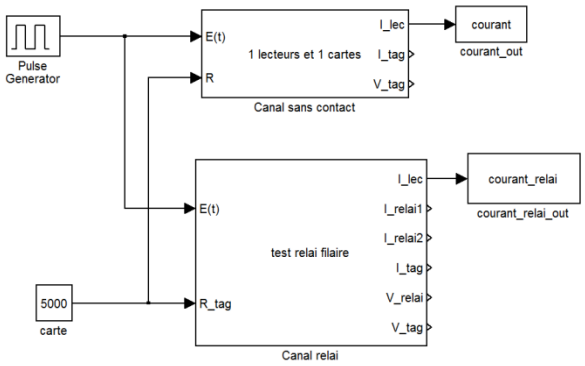


Figure IV-13 – modèles Matlab utilisés

On peut alors comparer les réponses temporelles au niveau de l'antenne lecteur dans différents cas. Dans un premier temps, il est intéressant d'identifier l'évolution du courant en

fonction du paramètre couplage entre les antennes. Dans le cas d'un relais filaire, il existe un couplage k_1 entre l'antenne lecteur et la première antenne du relais et un couplage k_2 entre l'antenne de la carte et la deuxième antenne du relais. En analysant de manière visuelle les courbes obtenues (figures IV-14 et IV-15), on remarque que le couplage qui influe le plus sur la réponse de la carte est le couplage du côté du lecteur. Sachant que le couplage entre la carte et l'antenne 2 du relais est très faible (l'attaquant n'est pas maître de cette distance), on peut dire que seul le couplage k_1 a une influence sur la réponse temporelle. La présence d'une carte sans contact à proximité du relais n'est pas indispensable pour détecter la présence du relais (on va prouver que cette détection est possible par la suite).

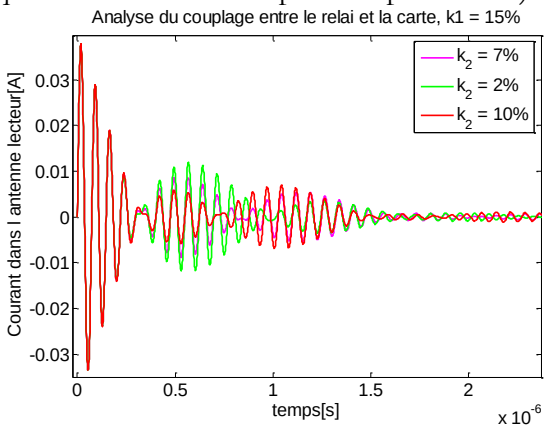


Figure IV-14 – Analyse des réponses en présence d'un relais en fonction du couplage au niveau de la carte (couplage lecteur 15%)

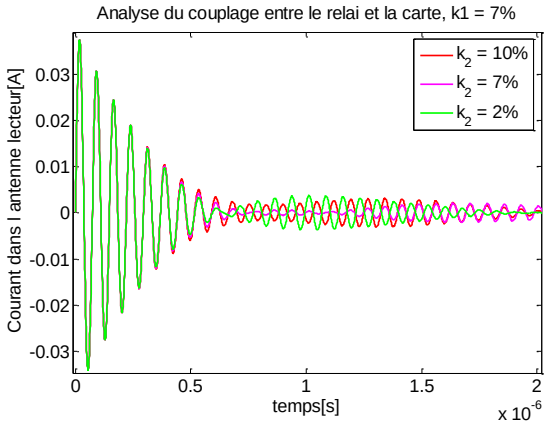


Figure IV-15 – Analyse des réponses en présence d'un relais en fonction du couplage au niveau de la carte (couplage lecteur 7%)

Il est aussi important de comparer la réponse à un échelon dans le cas d'un système sans contact classique avec celle d'un système dans lequel a été introduit un relais filaire. Il n'est pas intéressant d'analyser ces réponses pour un même couplage car les amplitudes des deux réponses sont trop différentes et la détection du relais est alors trop simple. Si on choisit deux réponses temporelles de même amplitude et forme, on remarque quand même un léger déphasage sur certaines oscillations du signal (figure IV-16). Un zoom sur les oscillations entre deux rebonds permet d'observer d'importantes différences entre les deux réponses (figure IV-17). Ces premières observations permettent de montrer qu'il est possible de détecter la présence d'un relais entre le lecteur et la carte en connaissant préalablement la réponse de la carte.

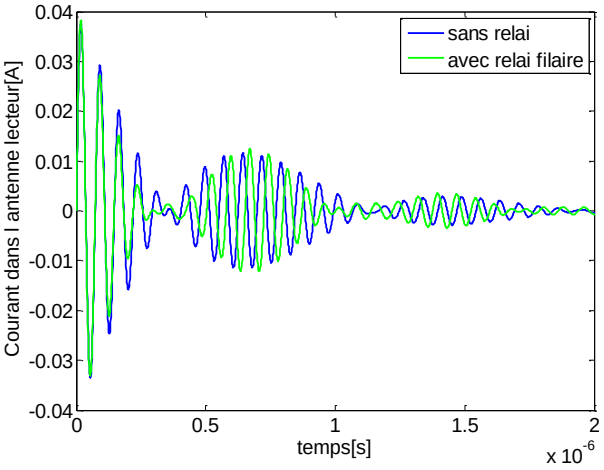


Figure IV-16 – Comparaison des réponses avec et sans présence d'un relais filaire (relais : couplage lecteur=20 %, couplage carte=10 % ; sans relais : couplage=10 %)

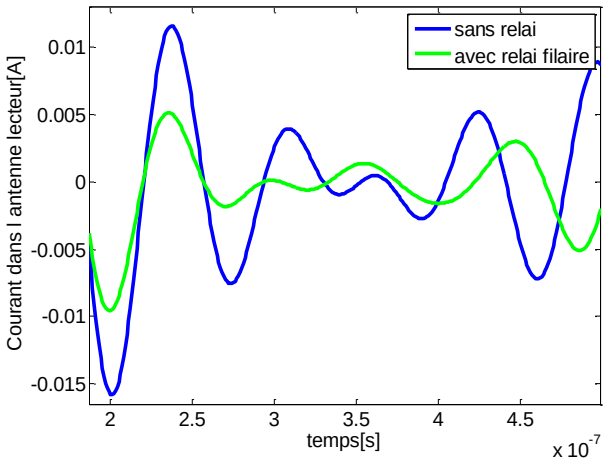


Figure IV-17 – Zoom sur le décalage de phase

Cette contre-mesure est basée sur la couche physique du système sans contact et donc difficilement contournable par un attaquant. En effet, les caractéristiques physiques d'une carte sont uniques puisque chaque carte sans contact possède son propre front-end RF (notamment l'antenne et la pompe de charge).

D. Soustraction de la réponse impulsionnelle

Les rebonds observés dans les différentes réponses à un échelon font penser à un écho provenant de la carte. Cet écho dépend très probablement des caractéristiques de la carte sans contact et du couplage entre les deux systèmes. Pour mettre en évidence cet écho, il suffit de soustraire la réponse d'un système (présence carte et/ou relais) à celle obtenue uniquement avec le lecteur. Les figures IV-18 et IV-19 montrent les échos obtenus en présence d'une carte sans contact et d'un relais pour différents couplages. On remarque que plus le couplage est important et plus les rebonds ont des temps de montée rapides. La bande passante du système global dépend du couplage entre les antennes. La différence est visible sur les différents sauts de phase. Dans le cas d'un système classique, les sauts de phases sont brefs et il est possible de distinguer différents échos (dans le cas de couplage important). Dans le cas du relais filaire, il devient difficile de distinguer ces différents rebonds. Plus le couplage est faible et plus il sera difficile de détecter la présence d'un relais ou d'une carte.

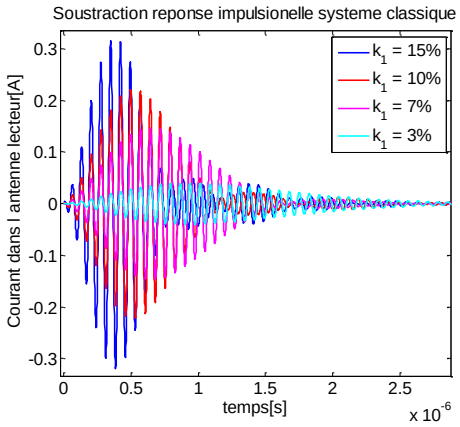


Figure IV-18 – Soustraction des réponses pour un système sans contact

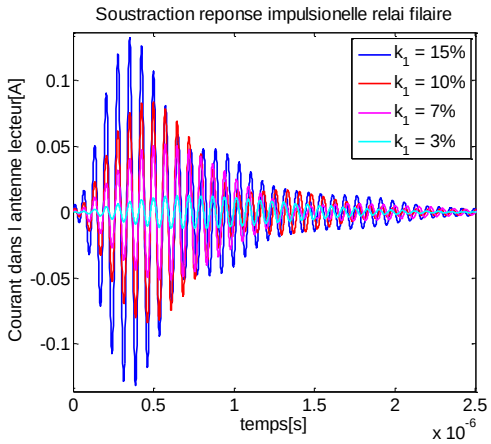


Figure IV-19 – Soustraction des réponses pour un système relais filaire

Pour vérifier que l'écho vient effectivement de la carte, il suffit de récupérer le courant au niveau de la carte lorsqu'un échelon se produit au niveau du lecteur. On réinjecte ensuite ce courant dans un modèle Matlab dont les entrées sont le courant de la carte (voir figure IV-20). On compare alors deux signaux :

- Le courant au niveau du lecteur lorsque le courant récupéré au niveau de la carte est injecté en entrée.
- La soustraction du courant au niveau du lecteur hors présence d'une carte avec celui en présence d'une carte.

Les figures IV-21 et IV-22 montrent que les deux signaux comparés et correspondant à l'écho sont identiques. On remarque uniquement un déphasage entre les deux signaux correspondant aux temps de traitement des différents modèles.

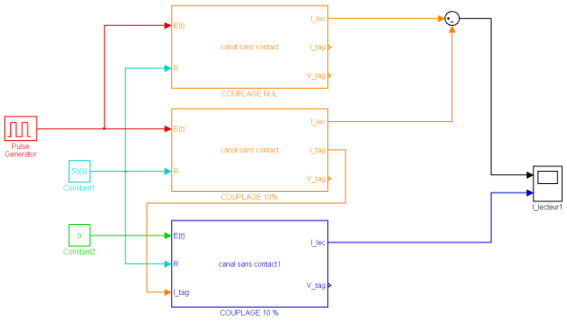


Figure IV-20 – modèle Matlab

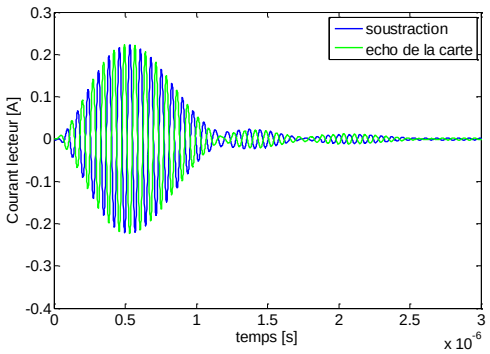


Figure IV-21 – Comparaison entre l'écho et la soustraction des réponses pour un couplage de 10%

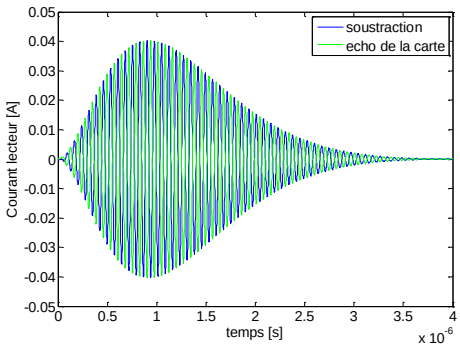


Figure IV-22 – Comparaison entre l'écho et la soustraction des réponses pour un couplage de 3%

Il y a donc un lien très étroit entre les différents rebonds observés et la soustraction du signal à une réponse impulsionnelle obtenue sans présence d'une carte.

3. Solution

L'objectif principal de la solution est de mesurer certains paramètres du système sans contact lorsqu'une carte ou un relais est à proximité du lecteur et que le couplage entre les deux éléments est suffisant pour établir une communication. Pour réaliser cette solution, trois phases sont essentielles : une phase de calibration, une phase de recherche et une phase de décision (voir figure IV-24). La phase de calibration permet d'acquérir les caractéristiques d'une réponse indicielle ou impulsionnelle qui seront utilisées comme références pour la phase de décision. Pour la phase de recherche, il s'agit d'une phase pendant laquelle le lecteur récupère une nouvelle réponse impulsionnelle correspondant à l'instant présent. Enfin, lors de la phase de décision, le lecteur est capable de conclure sur la présence d'un récepteur à partir des différents paramètres mesurés.

A. Phase de calibration

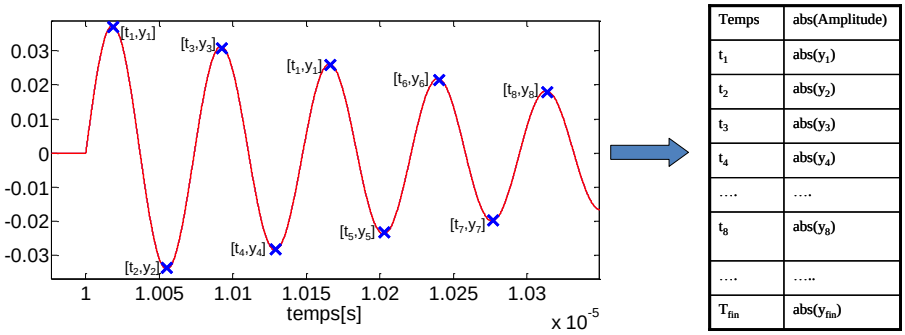
L'objectif de cette phase est de déterminer la réponse indicielle ou impulsionnelle du système sans la présence de récepteur inductif et avec la présence d'une ou plusieurs cartes valides. Le champ du lecteur n'est pas actif puisque dans notre solution, le champ RF n'est activé que lorsqu'une carte est à proximité du lecteur et qu'elle a été détectée. Le lecteur envoie donc un signal indiciel ou impulsionnel dans son antenne et récupère la réponse à ce signal. La forme de ce signal est une sinusoïde amortie comme nous l'avons précisé précédemment lorsque la carte n'est pas présente. Lorsque la carte est présente, on obtient des réponses différentes selon la distance entre les antennes. Un tel système est invariant dans le temps, le signal de réponse est le

même si les éléments composant le système n'évoluent pas (nous parlons ici principalement de l'antenne). Cette phase est donc réalisée une seule fois, lors de la mise en place du système.

L'analyse de la réponse indicielle ou impulsionnelle peut être réalisée par tous les moyens actuels permettant de caractériser un signal (caractérisations fréquentielles ou temporelles).

Exemple d'analyse et d'enregistrement de signaux :

Le signal à analyser est une sinusoïde amortie. Une première étape consiste à échantillonner le signal sur ses extremums. Ces extremums sont récupérés de manière synchrone avec le signal. L'horloge d'échantillonnage est le signal de réception. En numérisant le signal, on récupère à chaque front montant de l'horloge d'échantillonnage un couple de valeur correspondant à une valeur en temps (dont la référence est l'émission de l'échelon) et une valeur d'amplitude (voir figure IV-23).



Temps	abs(Amplitude)
t_1	abs(y_1)
t_2	abs(y_2)
t_3	abs(y_3)
t_4	abs(y_4)
….	….
t_8	abs(y_8)
….	…..
T_{fin}	abs(y_{fin})

Figure IV-23 – Echantillonnage sur les extremums de la réponse

Ces données sur les caractéristiques de la réponse obtenue sont sauvegardées dans un tableau, elles seront utilisées pour conclure quant à la présence d'une carte à proximité du lecteur.

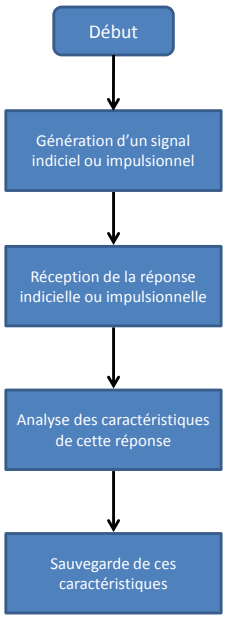


Figure IV-24 – Protocole d'analyse des réponses

B. Phase de recherche

Cette phase est sensiblement identique à la phase de calibration dans le sens où les étapes sont les mêmes. Pendant cette phase, le lecteur émet un signal indiciel ou impulsionnel dans l'antenne et récupère la réponse à ce signal. Pour cela, il détermine puis enregistre les caractéristiques de cette réponse dans un nouveau tableau de données. La principale différence est que cette phase peut être répétée dans le temps. La durée temporelle entre deux phases de recherche dépend de l'application et doit être définie par le propriétaire du système (de 10 µs à quelques ms).

C. Phase de décision

Lors de cette phase de décision, le lecteur compare les données obtenues à partir de la phase de recherche avec les données obtenues lors de la phase de calibration (comparaison du tableau créé lors de la calibration et du tableau créé lors de la phase de recherche).

Voici les différentes techniques qui peuvent nous permettre de comparer la réponse avec le signal de référence

- Corrélation des signaux
- Analyse de l'amplitude du signal par rapport à un seuil fixe
- Analyse spectrale
- Analyse statistique (variance, moyenne,….)

Si on observe des données sensiblement équivalentes avec les données de référence d'une carte valide, le lecteur conclut sur la présence d'une carte valide. Dans le cas contraire, le lecteur peut conclure sur la présence d'un relais ou d'une carte non valide et il n'active pas son champ RF.

4. Expérimentations

A. Le banc de test

Un exemple de réalisation a été mis en place pour valider cette étude théorique (figure IV-25). Son objectif principal est de mesurer l'influence d'une carte sans contact sur une antenne à boucle inductive et de comparer les réponses indicielles dans ces différents cas.

Lors de ces expérimentations, nous avons utilisé un générateur de signaux Tektronix AFG 3022 permettant l'envoi de signaux échelons paramétrables. Ce générateur est relié à une antenne compatible avec la norme ISO10373-6 et possédant un facteur de qualité de 10. Un oscilloscope Tektronik TDS5054 est utilisé pour visualiser et enregistrer le signal échelon d'onde (utilisé comme trigger) et le courant dans l'antenne de lecteur.

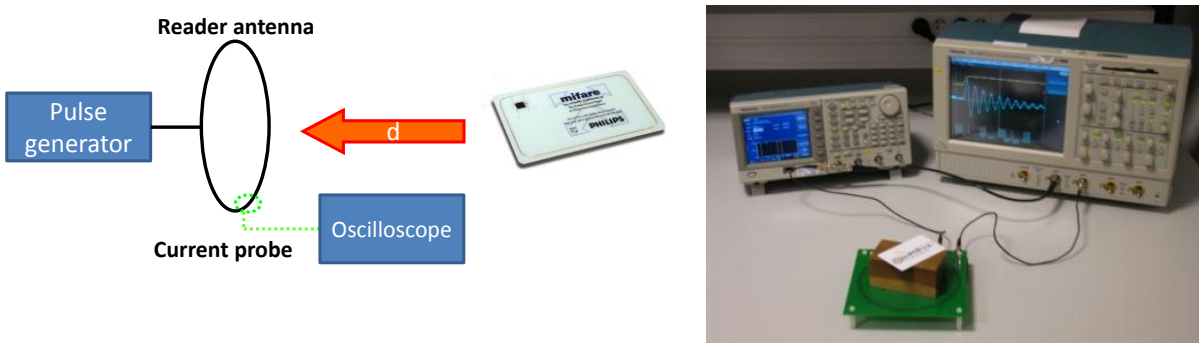


Figure IV-25 – Systèmes de mesures

Pour extraire la réponse échelon de notre système sans contact, une sonde de courant a été développée (voir figure IV-26). Ce système de récupération du courant dans l'antenne est basé sur le principe des pinces ampéremétriques. Le conducteur traversé par le courant est entouré d'un tore bobiné utilisé comme transformateur. Le courant dans le conducteur génère un champ magnétique dont les lignes de champ se regroupent sur le tore magnétique. La sonde de courant fournit une mesure proportionnelle au nombre de spires de son bobinage. Ce bobinage a été réalisé de façon à avoir un rapport 1.1 A/V entre le courant et la tension récupérée sur une charge 50 Ω (l'oscilloscope). Toutes les courbes données par la suite sont donc une image du courant en tension.

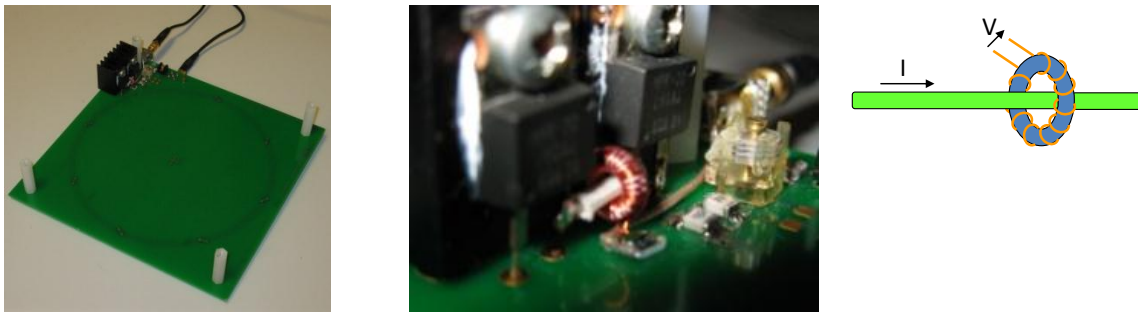


Figure IV-26 – Sonde de courant utilisée

B. Mesure du couplage entre lecteur et carte

Différents scénarios ont été évalués pour étudier l'impact d'une carte sans contact sur la réponse échelon de façon à vérifier l'influence du couplage sur le courant au niveau de l'antenne lecteur. Cette première expérience a été réalisée avec une carte sans contact compatible avec la norme ISO 14443-B pour analyser la réponse échelon pour différentes distances entre le lecteur et l'antenne de la carte Les oscillations sont enregistrées sur l'oscilloscope et comparées sous le logiciel Matlab. Les oscillations obtenues dans le cas « sans carte » sont utilisées comme référence.

Les courbes de la figure IV-27 décrivent la réponse échelon pour différentes distances entre l'antenne lecteur et l'antenne carte. Les résultats montrent une importante influence de la distance sur la forme du courant dans l'antenne lecteur. En réalité, ces oscillations ne dépendent pas de la distance, mais du couplage entre les deux antennes, comme cela a été observé lors des simulations. Cependant, le couplage dépend dans certains cas de la distance entre le lecteur et la carte sans contact.

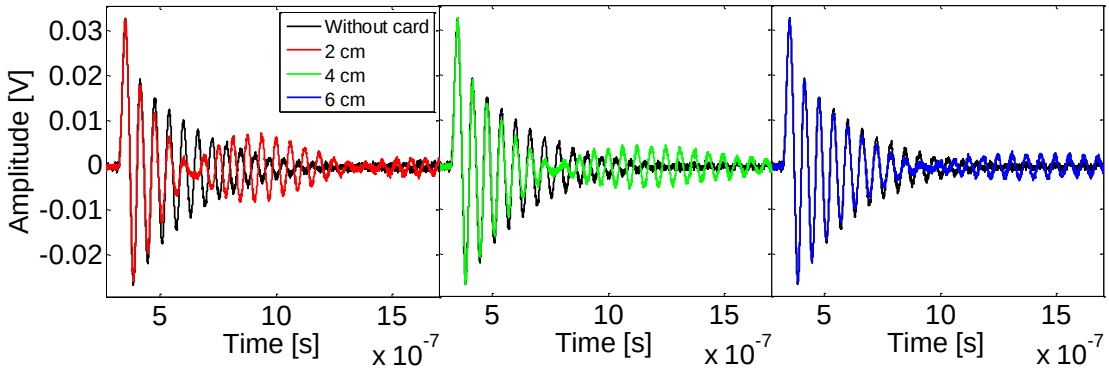


Figure IV-27 – Réponses obtenues pour différentes distances entre les antennes

On retrouve des résultats à peu près similaires avec la simulation ; les différences sont introduites par un modèle Matlab d'antennes dont les caractéristiques ne sont pas identiques à celles de l'antenne utilisée pour les expérimentations (l'antenne lecteur n'est pas un simple circuit RLC série et on ne connait pas les caractéristiques de l'antenne des cartes du commerce) (Figure IV-28 et IV-29).

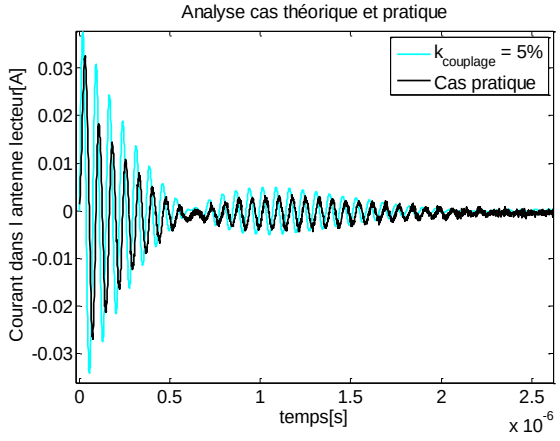


Figure IV-28 – Correspondance entre cas théorique (couplage de 5%) et cas expérimental (carte sans contact à 5 cm du lecteur)

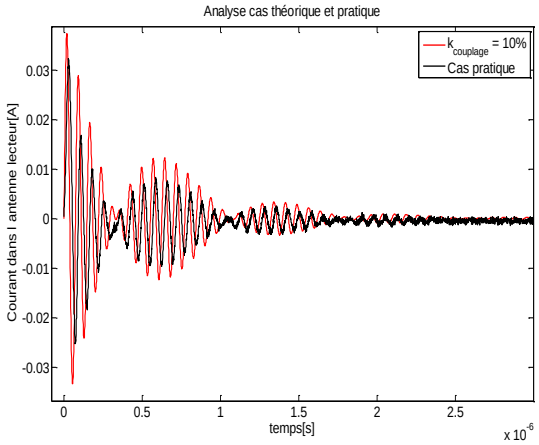


Figure IV-29 – Correspondance entre cas pratique (couplage de 10%) et cas expérimental (carte sans contact à 0 cm du lecteur)

C. Détection du type carte

La deuxième expérience consiste à comparer les réponses temporelles à un échelon de différentes cartes sans contact (voir figure IV-30). Chacune de ces cartes est compatible avec une norme sans contact à 13.56 MHz. Les trois différentes cartes sans contact utilisées sont :

- Une carte sans contact Inside Contactless compatible avec la norme ISO 14443-B
- Une carte sans contact Mifare NXP compatible avec la norme ISO 14443-A
- Une carte sans contact compatible avec la norme ISO 15693

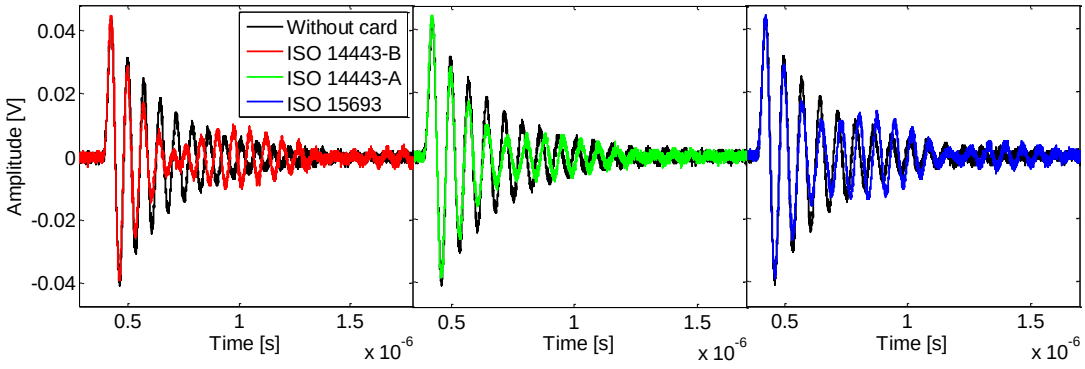


Figure IV-30 – Comparaison entre réponses obtenues pour des cartes de différents standards

La figure IV-30 décrit le comportement de la réponse à un échelon pour les trois différentes cartes. Chacune de ces réponses est comparée avec la réponse obtenue dans un cas sans aucune carte à proximité du lecteur. Les résultats montrent que la plupart des cartes sans contact semblent modifier la réponse à un échelon d'un système sans contact (quel que soit le standard utilisé). Cette altération de la réponse temporelle peut permettre de détecter la présence de cette carte à proximité du lecteur. Les cartes sans contact utilisant la norme ISO 14443-A sont cependant plus difficiles à détecter car on n'observe pas de rebond mais seulement une légère modification de l'amplitude et/ou de la phase dans la réponse temporelle. Le front-end RF utilisé par les cartes sans contact de type ISO14443-A est donc différent des autres standards. Cette particularité peut être expliquée par la forme des modulations qu'une telle carte est capable de démoduler (modulation OOK). Cette modulation à base de trous de champs nécessite un front-

end spécifique pour continuer d'avoir de la puissance et une horloge lorsque le champ du lecteur est éteint.

D. Détection de relais

Pour cette expérience, nous avons utilisé un relais filaire conforme avec le modèle simulé à l'aide de Simulink. Ce relais est simplement constitué d'un câble coaxial de longueur 1 m et de deux antennes type ID1 de coefficient de qualité 14 dont la fréquence de résonance est de 13.56 MHz (figure IV-31). Le relais est positionné entre un lecteur et une carte sans contact du commerce. Le lecteur et la carte sont de marque Inside Contactless et compatible avec la norme ISO14443-B.

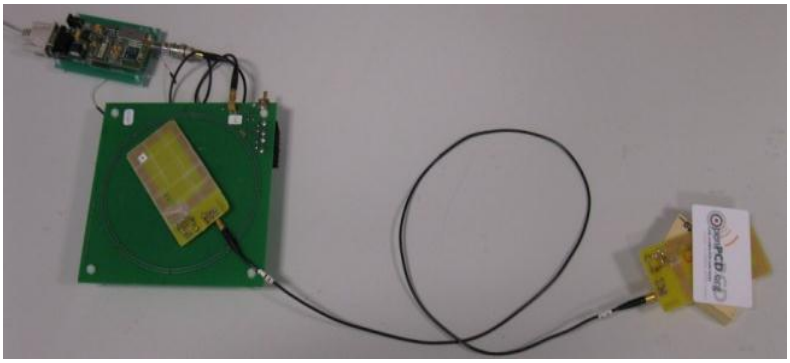


Figure IV-31 – Le relais filaire utilisé

En théorie, lorsque le couplage entre l'antenne du lecteur et l'antenne du relais est assez important, le couplage entre l'antenne relais et l'antenne de la carte a un impact sur la réponse du système global. Cependant, les tests en pratique ont montré que la présence de la carte n'influait pas vraiment sur la réponse temporelle du système. Toutes les réponses à un échelon d'un système avec relais ont donc été enregistrées dans un cas sans présence de carte sans contact (uniquement lecteur et relais).

Les figures IV-32, IV-33 et IV-34 montrent que les courbes obtenues par simulation pour un couplage donné peuvent être mises en relation avec une courbe obtenue par expérimentation à une distance donnée. Les courbes mises en relation ne sont pas choisies pour avoir la même amplitude mais pour avoir le rebond au même moment. On ne retrouve pas les mêmes amplitudes car le modèle Simulink utilisé n'est pas exact. On retrouve des couples couplage-distance assez proches pour le système sans contact simple et le système avec présence d'un relais. C'est-à-dire qu'un couplage de 10% correspond à une distance de 0 à 1 cm et un couplage de 5% est proche d'une distance de 5 cm.

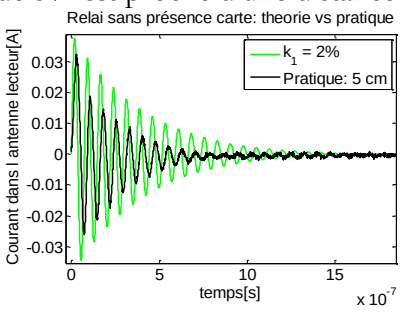


Figure IV-32 – Correspondance entre cas théorique (couplage entre les antennes de 2%) et cas expérimental (antenne du relais à 5 cm du lecteur)

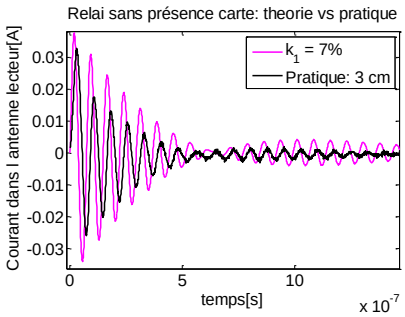


Figure IV-33 – Correspondance entre cas théorique (couplage entre les antennes de 7%) et cas expérimental (antenne du relais à 3 cm du lecteur)

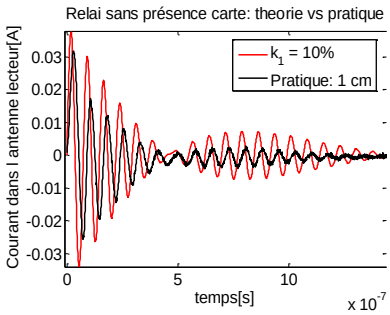


Figure IV-34 – Correspondance entre cas théorique (couplage entre les antennes de 10%) et cas expérimental (antenne du relais à 1 cm du lecteur)

Pour une même distance, un lecteur peut facilement détecter la présence d'un relais car la réponse à un échelon sera vraiment différente. Les figures IV-35 et IV-36 montrent la réponse obtenue pour deux distances identiques (2 cm et 6 cm) dans le cas d'un système sans contact classique et dans le cas d'un système avec relais. On observe de très importantes différences entre les réponses obtenues. Cette différence peut s'expliquer par le fait que la carte sans contact et le relais n'ont pas des antennes de même coefficient de qualité. Il est difficile de savoir si ces différences d'amplitudes sont dues seulement au coefficient de qualité ou à la présence du relais. Cependant, le relais filaire ne fonctionne pas lorsque le coefficient de qualité est proche de celui de la carte donc il est difficile de le tester dans ces conditions.

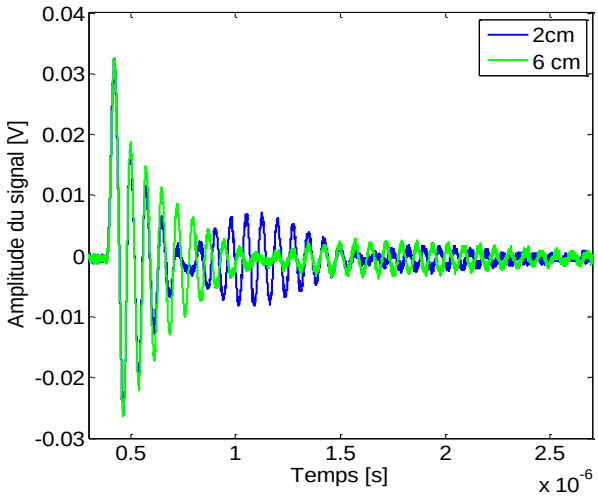


Figure IV-35 – Réponses d'un système sans contact

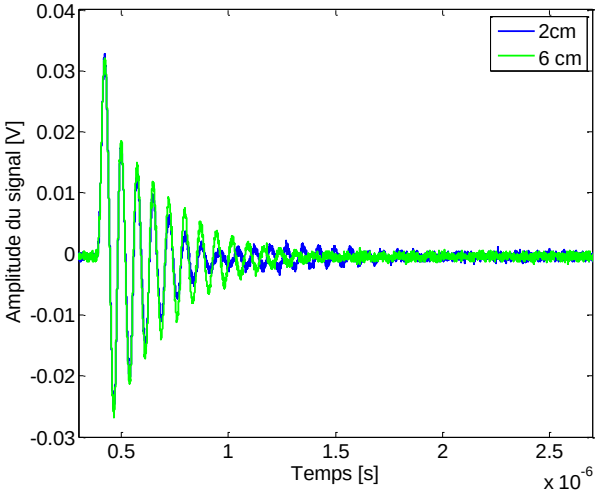


Figure IV-36 – Réponses d'un système avec présence d'un relais filaire

E. Analyse de l'écho

Les différentes simulations menées pendant la première étape de notre travail ont permis de montrer que c'est la réponse de la carte qui modifiait la réponse du lecteur. Nous avons observé que le signal renvoyé par la carte et reçu par le lecteur correspondait à la soustraction de la réponse obtenue sans carte avec celle obtenue à proximité d'une carte.

Il est donc intéressant de voir si l'on retrouve des résultats identiques lors d'expérimentations pratiques. Notre analyse nécessite trois phases expérimentales (figure IV-37) :

1. Le générateur de signal délivre un échelon et l'injecte dans une antenne de type lecteur (conformité avec la norme ISO 10373-6). Aucune carte sans contact ou antenne n'est présente en face de cette antenne lecteur. Le signal récupéré sur la sonde de courant de l'antenne lecteur est enregistré (signal A).
2. Le générateur de signal génère un échelon et l'injecte dans une antenne de type lecteur. Une antenne connectée à un oscilloscope en 50 Ω est positionnée à 0 cm de cette antenne lecteur. La carte est placée en couplage fort avec le lecteur de façon à obtenir des échos de forte amplitude. Deux antennes de type cartes sans contact ont été utilisées ; l'une possède un coefficient de qualité Q=188, l'autre un coefficient de qualité Q=22. Le signal récupéré sur la sonde de courant de l'antenne lecteur (signal B) et au niveau de l'antenne de type carte sans contact (signal C) est enregistré.
3. Le signal C enregistré est converti à l'aide du logiciel Tektronix ArbExpress. Il est alors possible d'utiliser le vecteur de données enregistré sur l'oscilloscope pour créer un signal compatible avec notre générateur de signal. Il est alors possible de réinjecter le signal C dans l'antenne de type carte sans contact de façon à récupérer le signal au niveau du lecteur (signal D).

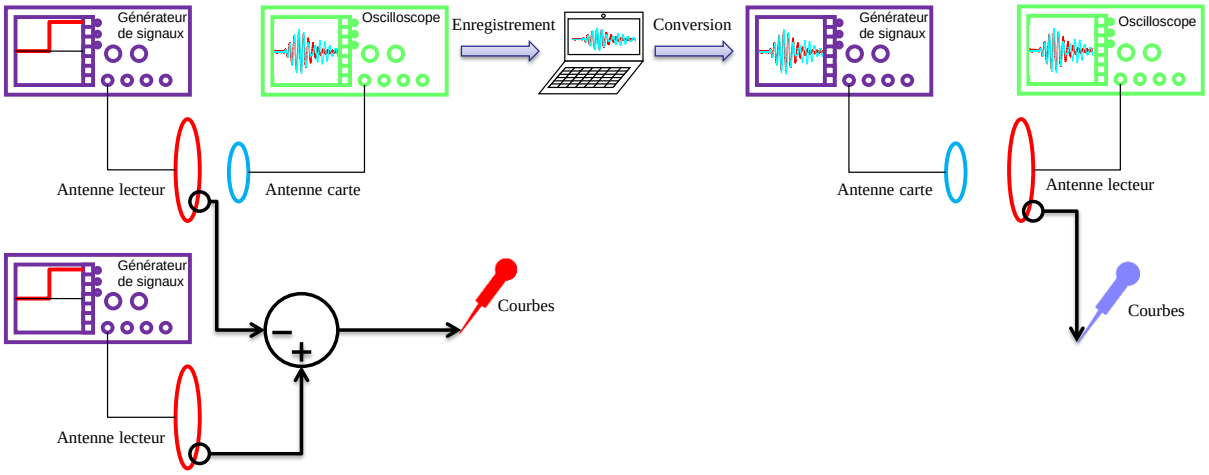


Figure IV-37 – Analyse de l'écho

Enfin, on compare sous Matlab la soustraction du signal A et du signal B avec le signal D.

On peut observer sur les figures IV-38 et IV-39 la comparaison de ces deux signaux pour des antennes de coefficients de qualité de valeur 22 et 188.

Seul le premier écho est intéressant. On note des formes assez similaires, en particulier la durée de l'écho, mais également d'importantes différences d'amplitudes pour l'antenne de coefficient de qualité Q=22. Il est possible d'expliquer cette différence par le changement de source et de récepteur entre la phase 2 et la phase 3. En effet, la source est d'abord connectée à l'antenne lecteur puis à l'antenne carte. La charge du récepteur est le 50 Ω de l'oscilloscope. L'oscilloscope et le générateur de signaux n'ont pas les mêmes circuits internes et peuvent donc créer des différences entre les signaux enregistrés.

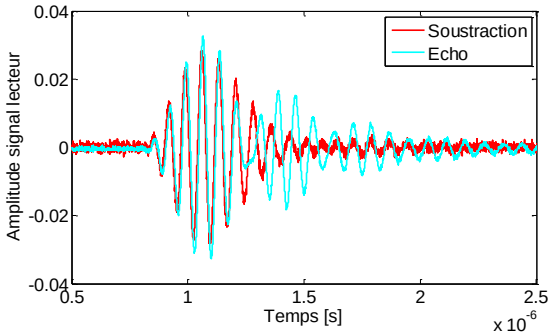


Figure IV-38 – Comparaison de l'écho et de la soustraction du signal au niveau du lecteur avec une carte de coefficient de qualité Q=188

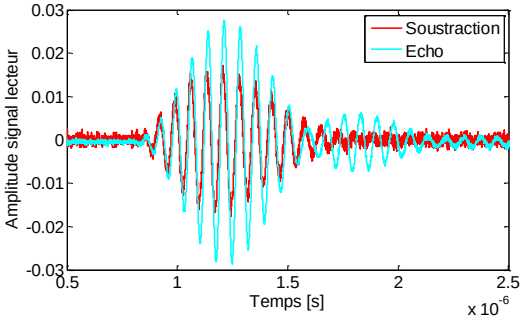


Figure IV-39 – Comparaison de l'écho et de la soustraction du signal au niveau du lecteur avec une carte de coefficient de qualité Q=22

5. Avantages de cette solution et travaux futurs

A. Avantages

a. Puissance consommée

Cette solution est très intéressante en termes de consommation d'énergie. Le lecteur n'a pas besoin d'activer son champ RF. L'expression mathématique d'une réponse à un échelon est décrite par l'équation IV-5.

$$i(t) = I_{max} e^{-\Delta t} \cos(\omega t) \qquad \text{(IV-5)}$$

L'énergie dissipée dans la résistance du lecteur lors d'un échelon peut être calculée en intégrant la puissance instantanée de cette résistance dans le temps (équation IV-6).

$$E = \int_0^\infty Ri^2(t)\,dt = R\int_0^\infty (I_{max}e^{-\Delta t}\cos(\omega t))^2\,dt = \frac{1}{2}RI_{max}^2\frac{\theta}{2}\left(\frac{1}{1+\theta^2w^2}+1\right) \qquad \text{(IV-6)}$$

La valeur d'Imax n'est pas connue parce qu'elle dépend de l'amplitude de l'échelon. Cette valeur peut être mesurée avec la sonde de courant : nous avons mesuré Imax = 0.033 A lors de nos expérimentations pour une antenne avec R = 2 Ω. L'énergie dissipée dans la résistance est proche de 0.13 nJ à chaque fois que l'on utilise notre solution.

Cette solution peut aussi être utilisée pour détecter la présence d'une carte à proximité du lecteur sans activer le champ radiofréquence du lecteur. Pendant cette étude, on a observé que la présence d'un récepteur à proximité du lecteur introduisait une modification de la réponse à un échelon, mais aussi que la consommation d'énergie d'une telle solution était très faible. Il est intéressant d'utiliser cette propriété pour détecter la présence d'une carte en minimisant la consommation d'énergie par le lecteur. Pour comparer la consommation d'énergie des systèmes actuels lors de la détection d'une carte sans contact et celle nécessaire par notre solution, il suffit de mesurer le courant dans l'antenne du lecteur lorsque le champ radiofréquence est actif. Nous avons mesuré un courant de 0.75A sur un lecteur du commerce de marque Inside Contactless. La consommation énergétique d'un lecteur dont le champ est actif en permanence est de 2 kJ. La différence de consommation est très importante ; l'utilisation de la réponse à un échelon pour détecter la présence d'une carte semble donc une solution d'avenir.

b. Autres avantages

Un autre avantage est que cette solution est très rapide puisque la durée des oscillations est en général inférieure à 2 µs. Après cette durée, le lecteur analyse la réponse temporelle et conclut selon les paramètres obtenus.

Cette solution ne nécessite aucun ajout technologique au niveau de la carte. Au niveau du lecteur, il faut simplement développer le générateur d'échelon et le système analysant la réponse temporelle.

Il n'est pas nécessaire de modifier les normes sans contact existantes pour utiliser notre solution puisqu'il n'est pas nécessaire d'activer le champ radiofréquence et d'envoyer de véritables requêtes.

Notre système ne perturbe pas de possibles lecteurs voisins, car le champ RF n'est pas activé.

B. Travaux futurs

Il est en premier lieu nécessaire d'implémenter complètement notre solution de façon à tester son fonctionnement sur un système sans contact du commerce. Pour cela, il sera nécessaire de réaliser un générateur d'échelon possédant des caractéristiques précises, en particulier un temps de montée très court (proche de 10 ns). Tout le système de récupération de la réponse et de son analyse doit être développé. Ce système inclut une sonde de courant et son circuit d'instrumentation de façon à obtenir une réponse de forte amplitude et très précise. Cela comprend aussi un système d'analyse (microcontrôleur, DSP, FPGA) permettant de sauvegarder certaines réponses de référence et de faire de la comparaison de réponse par corrélation, analyse spectrale,…

Une autre solution à étudier est l'analyse de la réponse impulsionnelle par la carte, c'est-à-dire étudier les signaux en sortie d'antenne de la carte lorsqu'un échelon est injecté dans l'antenne du lecteur.

Il est possible d'imaginer aussi une cartographie de différentes réponses impulsionnelles lorsqu'un utilisateur approche la carte de façon à réaliser une étude complète et en déduire les différentes propriétés de la réponse à l'échelon.

6. Conclusion

Ce travail est l'esquisse d'un énorme travail qui peut être réalisé sur la détection de carte, la mesure de couplage, l'authentification de manière physique d'une carte et la détection de relais de type « amplify and forward ». Une première analyse a permis de trouver de nombreux résultats basés sur de la théorie, des simulations et des expérimentations. Ces résultats ont permis de développer une solution basée sur la réponse à un échelon d'un système sans contact. Cette solution permet de différencier d'une part la réponse d'un système sans carte par rapport à un système avec carte mais aussi de mesurer le couplage entre cette carte et le lecteur. La mesure de ce couplage peut donner une indication au lecteur sur la proximité de la carte et donc de détecter les attaques de type « distance fraud ». Dans le cas d'un système NFC, le destinataire peut effectuer cette analyse de façon à vérifier que l'initiateur ne tente pas de réaliser une attaque skimming (activation de la carte de la distance). Chaque front-end de carte sans contact est unique puisqu'aucune antenne ni pompe de charge ne peut être strictement identique (dû au processus de fabrication), on peut donc penser qu'il est possible d'utiliser la réponse à un échelon pour authentifier une carte. Dans ce cas, la solution est basée sur la couche physique et donc très difficile à casser. De la même façon, notre procédé peut être utilisé pour détecter certaines attaques relais ou au moins rendre cette attaque plus complexe.

On peut imaginer que la carte sans contact soit capable d'analyser le signal reçu sur son antenne lorsqu'un échelon est injecté sur l'antenne lecteur même si cela n'a jamais été testé. Il est alors possible de développer un protocole d'authentification basé sur les différentes solutions.

PARTIE II. SOLUTION BASEE SUR LE BRUIT

Dans cette partie, nous étudions la possibilité d'utiliser la couche physique d'un canal sans contact ou sans fil pour détecter les attaques relais. Les attaques relais appelées aussi 'trou de ver' dans les réseaux sans fil et mobiles deviennent plus sophistiquées. Il est très difficile de détecter de telles attaques, particulièrement les relais de type « amplify and forward », en utilisant les méthodes existantes. Nous proposons une solution basée sur les caractéristiques de la couche physique des communications sans fil. Cette solution vise à détecter les variations statistiques de bruit lorsqu'une communication par le biais d'un relais se produit. Ces variations de bruits peuvent être analysées par le front-end RF existant dans les systèmes actuels. Ainsi, aucune modification hardware n'est nécessaire pour détecter les attaques relais et aucune modification des standards ou protocoles existants n'est exigée. Cette solution convient à la plupart des systèmes sans fil et sans contact. Pour évaluer l'efficacité de notre solution contre les attaques de relais, nous avons réalisé plusieurs campagnes de mesures sur des systèmes sans contact du commerce dans un environnement non protégé contre les perturbations d'autres systèmes électromagnétiques. Nos résultats ont montré qu'il était vraiment difficile de caractériser le bruit d'un système sans contact et de comparer différents bruits. La raison principale de cette difficulté à trouver l'empreinte d'un système est la non-linéarité du canal sans contact. La solution a ensuite été implémentée sur un système sans contact d'expérimentation. Cette étude a permis de montrer qu'il était possible d'identifier un récepteur sans contact à condition de connaître certains paramètres du système (le couplage par exemple). Le travail proposé a fait l'objet d'une collaboration avec un spécialiste des réseaux de capteurs.

1. Etat de l'art

A. Introduction aux réseaux de capteurs

Depuis des dizaines d'années, les capteurs se développent dans de nombreux domaines d'applications : industriels, environnementales,... Ces dispositifs permettent de collecter et de transmettre des données physiques (T°, force, pression) vers une unité intelligente capable de traiter ces informations et de contrôler les paramètres physiques. Régulation de température, détection de fumée ou de présence sont autant d'applications permises par l'utilisation de capteurs. Auparavant, les données du capteur étaient acheminées par le biais d'un câble jusqu'au contrôleur qui prenait ensuite les différentes décisions. Suite aux progrès réalisés sur les différentes technologies sans fil, ce lien coûteux et encombrant a pu être remplacé par des liaisons radiofréquences. Aujourd'hui, les réseaux de capteurs permettent à un contrôleur de récupérer les données provenant d'une multitude de capteurs en utilisant uniquement les ondes radio (figure IV-40).

Figure IV-40 – Exemple de capteur sans fil

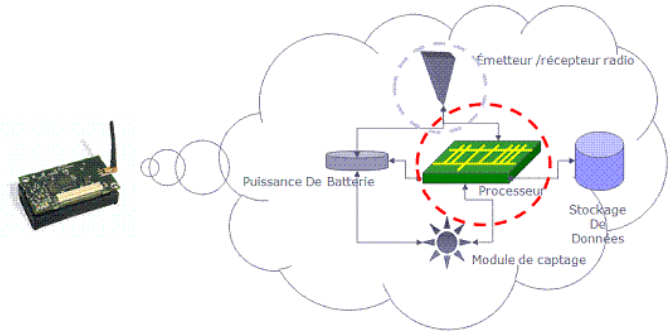


Figure IV-41 – Structure d'un capteur sans fil [TICE]

L'architecture d'un capteur utilisé dans les réseaux sans fil est généralement constituée de 4 unités de base : l'unité «sensible», l'unité de traitement, l'unité de transmission et l'unité de contrôle d'énergie (figure IV-41). L'unité «sensible» est le cœur même du capteur ; elle est basée sur un récepteur (le système générant un signal analogique à partir de la donnée physique) et un transducteur (le système traitant cette information analogique pour la convertir en donnée numérique). Le signal numérique obtenu est alors compréhensible par l'unité de traitement (microcontrôleur ou microprocesseur). Alors que l'unité « sensible » transforme des données de la couche physique, l'unité de traitement travaille au niveau des couches plus hautes et permet l'implémentation de protocole de communication et d'algorithmes de traitement et d'analyse de l'information. L'unité de transmission permet de gérer les communications entre l'émetteur et le récepteur et utilise généralement le lien radio. Il faut savoir qu'un nœud de réseau doit être autonome en énergie ; il utilise généralement une batterie mais peut aussi utiliser des systèmes de récupération d'énergie liée à son environnement (vibrations, chaleur, solaire,…). Ces ressources énergétiques sont donc très limitées et le capteur doit être capable de gérer de façon optimale cette énergie disponible pour garantir une durée de vie importante du capteur.

Un réseau de capteurs peut être constitué d'une multitude de nœuds utilisant les mêmes topologies d'architectures que les systèmes réseaux classiques. Une différence importante est la notion de passerelle ; l'ensemble des capteurs transmet ses données à un dispositif unique. Cette architecture permet de garantir le fonctionnement du réseau même lorsqu'un nœud est détérioré, mais aussi une collecte de données plus stable.

B. Etat de l'art des solutions utilisées pour les attaques relais (réseaux de capteurs et réseaux véhiculaires)

a. Réseaux de capteurs

Pour détecter l'attaque relais ou 'trou de vers' dans les réseaux coopératifs de type ad hoc ou de capteurs, deux principales approches ont été proposées dans la littérature.

Dans la première approche, un principe de fonctionnement, appelée « packet leashes », est utilisé pour limiter la propagation des paquets. Dans [HU2006, HU2004, WEI2006], deux mécanismes ont été proposés pour détecter l'attaque relais : *« temporal leashes»* et *«geographic leashes».* Ces paramètres permettent de déterminer la position de l'émetteur et de limiter le temps de propagation. Le paramètre *«temporal leashes»* permet de mesurer les retards en fonction du temps d'émission et de réception (y compris le temps de traitement du paquet). Cette solution exige l'utilisation d'horloges synchronisées pour réduire les erreurs de décisions. Quant au paramètre *«geographic leashes»* il a pour rôle de vérifier la position géographique de l'émetteur du paquet. L'inconvénient de ce mécanisme est qu'il nécessite l'utilisation d'un système GPS « Global Position System ».

Quant à la deuxième approche, elle est basée sur le temps de vol des paquets en utilisant « Round Trip message Time (RTT)». Dans [CAP2003, HU2003-B, KOR2005], les auteurs proposent de mesurer le temps nécessaire pour l'envoi d'un message et la réception de son acquittement appelé « Round Trip Travel Time ». Ce paramètre permet de mesurer le temps nécessaire pour qu'une impulsion de signal ou un paquet atteigne la destination et soit retransmis vers la même source. L'avantage de cette solution est qu'elle n'exige pas l'utilisation d'une horloge synchronisée. Toutefois, elle ne tient pas compte du temps requis pour le traitement d'un message. Quand un message est envoyé par un émetteur et retransmis par le récepteur, cette période de temps n'est pas négligeable.

De nombreuses autres solutions ont été proposées afin de détecter l'attaque relais ou de « wormhole » dans des environnements de communication bien particuliers. Dans [HU2003-A, LAZ2004], des antennes directionnelles ont été utilisées pour détecter l'attaque relais dans les réseaux ad hoc. Dans [WAN2004], une approche basée sur la mesure de distance entre voisins et utilisant la puissance du signal reçu a été proposée pour les réseaux de capteurs statiques. Dans [LAZ2005], une solution utilisant la théorie des graphes a été proposée mais celle-ci est peu adaptée aux réseaux mobiles. Les auteurs de [KHA2005] proposent que chaque émetteur/récepteur garde une table de voisins à deux sauts. Grâce à ces informations, les capteurs jouent le rôle de « chien de garde (watchdog) » et détectent ainsi la présence de l'attaque wormhole.

b. Réseaux véhiculaires

De nombreux brevets proposent des solutions pour lutter contre l'ouverture de voiture par attaque relais à l'insu du propriétaire. Dans les brevets [EP1650581, WO200635361, WO114227, WO0125060], les auteurs proposent des solutions utilisant en majorité la mesure du temps de transfert de l'information ou la localisation de la clé et utilisant en général plusieurs antennes. Cependant, des systèmes plus simples basés sur les ondes sonores sont aussi étudiés. Tous ces brevets ne peuvent pas s'appliquer à tous les systèmes sans fil, ils sont généralement étudiés pour le domaine automobile afin d'authentifier les clés et commander l'ouverture des portes ou le démarrage de la voiture.

Le brevet [US0255909] identifié lors de la recherche de brevets par l'INPI recense une solution très proche de la contre-mesure que nous avons développée. Cette solution a pour objectif de mesurer les interférences introduites par le relais au niveau de la base station. En effet un relais amplifie non seulement le signal utile (la porteuse du signal transmis) mais aussi des

fréquences de bruit dans la bande passante de l'amplificateur. Le bruit ambiant autour de la station de base augmente et celle-ci peut alors détecter un changement et conclure sur la présence d'un relais. Le principe de base de la solution est le même que celui que nous allons présenter dans la suite. Le principal ajout de notre solution est la phase de calibration.

C. Canal sans contact versus canal sans fil

Le canal de communication utilisé pour les communications sans contact est différent de celui utilisé pour les communications sans fil comme on peut le voir dans le tableau IV-1. Nous allons détailler dans cette partie les principales caractéristiques de ces deux modes de communication.

Tableau IV-1 – Comparaison entre champ proche et lointain

« Champ proche »	$< \frac{\lambda}{2\pi} <$	« Champ lointain »
Couplage magnétique		Propagation d'onde
Loi de Biot et Savart		Equation de Maxwell

La technologie sans contact est basée sur le couplage entre deux boucles inductives. Lorsqu'un courant est injecté dans la première boucle inductive, cette dernière génère un champ magnétique suffisant pour introduire un courant dans la deuxième boucle inductive (à condition que le couplage entre les deux bobines soit suffisant). La modulation de ce courant ou la modulation d'une charge aux bornes de cette boucle peut alors permettre la transmission de données entre les deux boucles. Ces deux boucles sont considérées comme des antennes ; elles sont adaptées et résonnent à la seule fréquence de 13.56 MHz. La distance de communication entre ces deux systèmes à boucles inductives est en général assez faible (inférieure au mètre) si le transpondeur utilise le champ magnétique comme source d'énergie. L'équation liant les différentes données est la loi de Biot et Savart qui est décrite par l'équation IV-7. Cette équation établit une relation entre le champ magnétique H et le courant I traversant un élément dl de circuit électrique de longueur l lorsque le point de mesure est à une distance x de l'élément.

$$\overrightarrow{dH} = \frac{I.\overrightarrow{dl} \wedge \vec{u}}{4\pi(x^2)} \tag{IV-7}$$

Les technologies sans fil sont basées sur l'émission d'ondes électromagnétiques et l'utilisation de dipôles électriques pour transmettre les signaux. De très nombreuses normes utilisent ces systèmes de transmission de données, en particulier les réseaux de capteurs. Alors que les systèmes sans contact utilisent les ondes HF et font partie des systèmes de communication en champ proche, les systèmes sans fil font partie des systèmes de communication en champ lointain. La fréquence de la porteuse est bien plus grande et la distance de fonctionnement peut dépasser plusieurs centaines de mètres. Les équations utilisées pour résoudre de tels systèmes sont les équations de Maxwell décrivant le champ électromagnétique créé par un dipôle (équations IV-8, IV-9, IV-10).

$$H_\theta = \frac{ISsin\theta}{4\pi r^3}\left(1 + j\frac{2\pi r}{\lambda} - \frac{4\pi^2 r^2}{\lambda^2}\right)e^{j2\pi rwt/\lambda} \tag{IV-8}$$

$$H_\varphi = \frac{IScos\theta}{4\pi r^3}\left(1 + j\frac{2\pi r}{\lambda}\right)e^{j2\pi rwt/\lambda} \tag{IV-9}$$

$$E_\varphi = j\pi\frac{ISsin\theta}{w\varepsilon_0\lambda^2 r^2}\left(1 + j\frac{2\pi r}{\lambda}\right)e^{j2\pi rwt/\lambda} \tag{IV-10}$$

2. Scénario d'attaques et analyse théorique

Pour transmettre des données entre un émetteur A et un récepteur B, l'attaquant peut utiliser différents types de relais. Dans cette partie, nous présentons les bases de notre solution pour les trois stratégies différentes qui peuvent être utilisées par un attaquant :

- retransmission directe sans amplification
- amplification et retransmission : « amplify and forward »
- décodage et retransmission : « decode and forward »

Ces scénarios ont été étudiés pour les systèmes sans fil.

A. 1er scénario : retransmission directe du message

Dans ce scénario, le système est composé d'un émetteur A, d'un récepteur B et d'un relais R. Le relais R peut être équipé d'une ou plusieurs antennes émettrices/réceptrices (figure IV-42) : une pour la réception du signal envoyé par A et une autre utilisée pour la réémission du même signal (figure IV-43). Ces antennes peuvent être des antennes MIMO (Multiple Input Multiple Output), SISO (Single Input Single Output) ou bien MISO, SIMO.

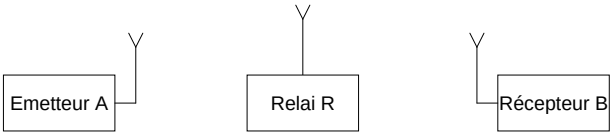


Figure IV-42 – 1er exemple de relais direct

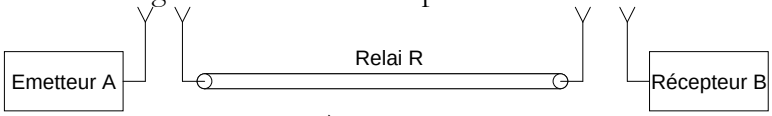


Figure IV-43 – 2ème exemple de relais direct

Pour cet exemple de scénario, l'émetteur A envoie un signal X à B. Si la transmission est réalisée par trajet direct ; le signal reçu par B s'écrit sous la forme suivante :

$$Y_{AB} = H_{AB}.X + N_B \qquad \text{(IV-11)}$$

avec H_{AB} la réponse du canal entre A et B et N_B un bruit blanc gaussien mesuré au niveau de B.

Cependant, si un intermédiaire placé entre A et B retransmet directement le signal envoyé par A vers B sans l'amplifier ; le signal reçu devient :

$$Y_{AB-R} = H_{RB}.H_{AR}.X + H_{RB}.N_R + N_B \qquad \text{(IV-12)}$$

avec H_{AR} (resp. H_{RB}) la réponse du canal entre A et R (resp. R et B) et N_R (resp. N_B) un bruit blanc gaussien mesuré au niveau de R (resp. B).

Les équations IV-11et IV-12 montrent une différence entre les quantités de bruit avec et sans relais (voir la partie en rouge de l'équation). L'objectif est de comparer les caractéristiques du bruit mesuré lors d'une phase de calibration et les caractéristiques du bruit mesuré lors d'une communication ; on devrait alors observer une différence de bruit et détecter la présence d'un relais.

B. 2ème scenario: amplify and forward

Dans ce scénario, on considère un système composé par un émetteur A, un relais R et un récepteur B. Le relais R dispose d'un amplificateur comme le montre la figure IV-44.

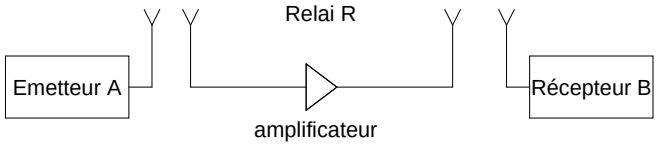


Figure IV-44 – Relais avec amplificateur

Le signal reçu par le relais est sous la forme suivante :

$$Y_{AR} = H_{AR}.X + N_R \quad \text{(IV-13)}$$

avec H_{AR} la réponse du canal entre A et R et N_R un bruit blanc gaussien mesuré au niveau de R. Le signal reçu par R est amplifié avec un gain G et retransmis à B, le signal reçu par B devient alors :

$$Y_{AB-R} = G.H_{RB}.H_{AR}.X + (G.H_{RB}.N_R + N_B) \quad \text{(IV-14)}$$

avec H_{AR} (resp. H_{RB}) la réponse du canal entre A et R (resp. R et B) et N_R (resp. N_B) un bruit blanc gaussien mesuré au niveau de R (resp. B).

D'après les équations IV-11 et IV-14, une différence entre les quantités de bruit est observée (termes en rouge).

C. 3ème scenario: "Decode and Forward"

Dans certains cas, l'attaquant est capable de décoder le message avant de le retransmettre à la destination. Ainsi, le message reçu par le récepteur B est sous la forme suivante :

$$Y_{AB-R} = H_{RB}.X' + N_B \quad \text{(IV-15)}$$

avec H_{RB} la réponse du canal entre R et B, X' le message décodé par R et N_B un bruit blanc gaussien mesuré au niveau de B.

En comparant les quantités de bruit des équations IV-11 et IV-15, on constate que B est incapable de détecter la présence de ce type de relais et suppose que le message a été transmis via un chemin à un saut. Des solutions basées sur la mesure des retards ont été proposées pour détecter ce type de scénario [HU2006, REI2006]. Cependant, ces techniques nécessitent des horloges synchronisées à l'émission et à la réception.

Notre solution propose alors que l'émetteur A ou le récepteur B ajoute avant l'envoi du message un bruit N_C dont les paramètres sont connus par les deux dispositifs communicants autorisés. Ainsi le message reçu par B et envoyé par A est défini par l'équation suivante :

$$Y_{AB} = H_{AB}.X + (N_C + N_B) \quad \text{(IV-16)}$$

avec H_{AB} la réponse du canal entre A et B , N_B un bruit blanc gaussien mesuré au niveau de B et N_C un bruit pré défini par A et B.

L'attaquant relais R décode le message et le retransmet à B. Ce dernier reçoit un message sous la forme IV-15. Les équations IV-15 et IV-16 montrent une différence des quantités de bruit. Ainsi le récepteur B est capable de détecter la présence d'un relais.

3. Solution envisagée

L'objectif principal de notre solution est de détecter la présence d'un ou plusieurs relais placés entre l'émetteur et le récepteur. Pour réaliser cette solution, trois phases sont nécessaires : une phase de calibration, une phase d'analyse et une phase de décision. La phase de calibration permet d'acquérir les caractéristiques d'un bruit de référence lorsqu'aucun relais n'est présent. Quant à la phase d'analyse, il s'agit de la phase habituelle d'échange des données entre A et B. Enfin, lors de la phase de décision le récepteur est capable de conclure sur la présence d'un relais dans le chemin de transmission. Nous présentons ici la solution générale pour tous les systèmes

sans contact et sans fil ; cette solution nécessite cependant quelques ajustements selon l'application et le standard sans fil utilisé.

A. Phase de calibration

Le but est de déterminer les caractéristiques du bruit pour une communication directe entre un émetteur et un récepteur autorisés sans la présence de relais. Cette phase doit donc être réalisée pendant une communication sans relais ou lorsqu'il n'y a pas de communication entre les deux parties (à vide), avant le déploiement du réseau.

La figure IV-45 montre un exemple de caractérisation du bruit pour une communication half duplex sans la présence de relais. Dans ce scénario, l'émetteur enregistre la réponse du récepteur (la simple présence d'un récepteur peut être considérée comme une réponse dans le cas d'un système sans contact). Après acquisition et filtrage de ce signal, l'émetteur caractérise le bruit.

Pour réaliser cette solution, il est possible d'utiliser tous les moyens d'analyse des signaux permettant de caractériser un bruit enregistré. Il existe de nombreuses façons de caractériser un bruit : des méthodes statistiques, des caractérisations de réponses fréquentielles ou temporelles. Toutes ces techniques peuvent permettre d'identifier le bruit enregistré et de pouvoir comparer différents bruits. Voici quelques exemples de méthodes de caractérisation du bruit :

- Corrélation des signaux
- Analyse de l'amplitude du signal par rapport à un seuil fixe
- SNR (Signal to Noise Ratio)
- Analyse spectrale
- Analyse statistique (variance, moyenne,…)

L'information qui concerne le bruit sera utilisée comme référence pour détecter si les transmissions suivantes ont été effectuées en présence ou non d'un relais.

B. Phase d'analyse

La phase d'analyse est sensiblement la même que la phase de calibration ; elle correspond à un enregistrement du bruit au niveau de l'émetteur. Après l'acquisition du signal, les caractéristiques du bruit sont mesurées et comparées aux informations acquises pendant la phase de calibration.

Le diagramme de la figure IV-47 montre la réalisation de la solution. Le lecteur récupère N échantillons à des moments aléatoires ou à des moments précis de la communication (ex : trous de champs en ISO14443-A). Les paramètres sont choisis en fonction de l'application, du niveau de sécurité des données transmises, de la différence trouvée entre les caractéristiques calculées et comparées. Parmi les paramètres, certains sont indispensables : la fréquence d'échantillonnage, le nombre d'échantillons à acquérir, la méthode utilisée pour obtenir les caractéristiques du bruit, …

C. Phase de décision

La phase de décision est très importante car elle doit décider en fonction des résultats s'il y a présence d'un ou plusieurs relais entre l'émetteur et le récepteur. C'est lors d'une ou plusieurs comparaisons entre les caractéristiques du bruit évaluées lors d'une communication et celles du bruit évaluées lors d'une phase de calibration que la décision va être prise. Le nombre de comparaisons effectuées dépend des résultats obtenus à chaque comparaison et de l'application. Des tests d'hypothèses peuvent aussi être utilisés pour réduire le nombre de fausses alarmes.

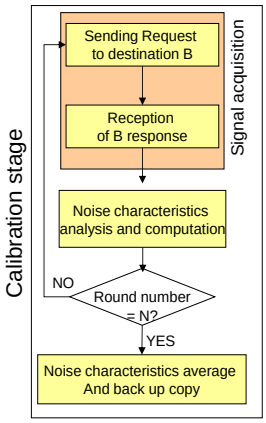


Figure IV-45 – Phase de calibration

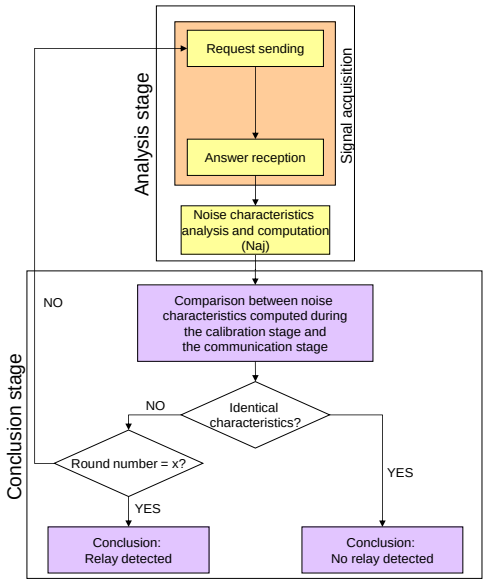


Figure IV-46 – Phase d'analyse et de conclusion

4. Premières expérimentations sur des systèmes sans contact

Comme nous l'avons évoqué dans l'introduction, l'objectif principal de notre solution est de mesurer l'influence du relais sur la puissance du bruit au niveau du lecteur ou au niveau de la carte et du lecteur. En effet, lors d'un échange direct entre un émetteur et un récepteur, le niveau de bruit est différent de celui mesuré lors d'un échange avec relais de l'information. On va donc comparer les niveaux de bruit dans deux cas : sans relais et avec relais. Nous avons donc étudié l'impact de différents paramètres sur le bruit : types de cartes, fréquence d'échantillonnage, types de relais.

Dans un premier temps, nous avons étudié des scénarios sans relais en faisant évoluer les paramètres de mesure. Cette phase sert de référence ; c'est la phase de calibration. Ensuite, nous étudions des scénarios avec la présence de différents relais de façon à analyser l'impact de leur intrusion sur le système. Nos expérimentations montrent la difficulté d'utiliser le bruit comme signature d'un système, en particulier dans le cas de systèmes sans contact.

A. Méthode d'analyse

Nous avons choisi d'utiliser les communications en champ proche et plus précisément la technologie sans contact pour valider nos hypothèses concernant la modification du niveau de bruit. Les signaux utilisés seront conformes à la norme ISO 14443-A lorsque cela n'est pas précisé. Notre banc de mesure est composé de (figure IV-47) :

- Le dispositif d'émission choisi est un lecteur Inside Contactless.
- Le module de réception est une carte RFID NXP Mifare Classic.
- Outils de mesure : les bobines de calibration connectées à l'oscilloscope permettent d'enregistrer le signal. l'oscilloscope Tektronik TDS5054 employé lors des mesures permet d'échantillonner les signaux à 5GS/s.

La forme du relais varie selon les expériences ; ils seront détaillés dans les parties les concernant.

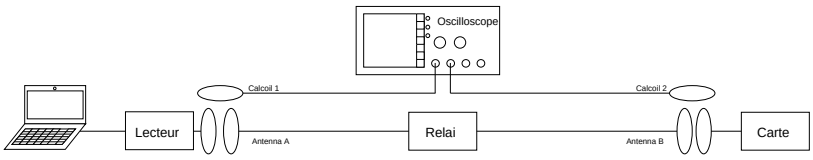


Figure IV-47 – Méthode d'expérimentation

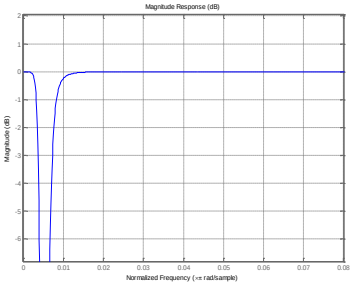


Figure IV-48 – Caractéristiques du filtre coupe-bande

Lors de chaque expérience, les signaux sont enregistrés sur l'oscilloscope. Ils sont alors importés sous Matlab pour être traités. Chaque signal est filtré de façon à ne récupérer que le bruit. Le signal utile est centré en 13.56 MHz et a une bande passante d'environ 2 MHz. On réalise un filtre coupe-bande pour filtrer les fréquences utiles ; ce filtre aura pour fréquences de coupure 9 MHz et 18 MHz (voir figure IV-48). On considère alors que le signal filtré ne contient que des fréquences correspondant à du bruit.

On réalise des histogrammes à partir des signaux filtrés pour analyser la répartition du bruit selon les cas de figures.

Quelques notations :

- Antenne A : antenne du relais côté lecteur
- Antenne B : antenne du relais côté carte

B. Influence des paramètres de l'analyse

a. Temps d'analyse

Cette première expérimentation consiste à démontrer que la durée d'analyse n'a pas un fort impact sur l'histogramme de bruit obtenu. Le lecteur envoie une requête à la carte sans contact sans présence de relais entre les deux dispositifs ; la carte sans contact répond à cette requête. Le signal HF correspondant à ces deux trames est enregistré au niveau de l'oscilloscope (Figure IV-49). Le signal est découpé en plusieurs vecteurs temporels de tailles différentes. Ces différents vecteurs d'échantillons correspondent à des temps d'analyse de différentes durées. On extrait le bruit de chacun de ces vecteurs en les filtrant puis on en déduit leurs histogrammes. La figure IV-50 montre les histogrammes de bruit pour les différents vecteurs. Comme on peut l'observer, la forme générale des différents histogrammes n'évolue pas Les différences d'amplitude observées correspondent uniquement à des vecteurs temporels différents et donc à un nombre d'échantillons différent. On en déduit donc que la distribution de bruit ne dépend pas du temps d'acquisition.

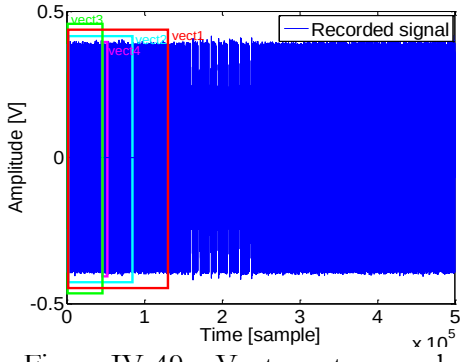


Figure IV-49 – Vecteurs temporels analysés

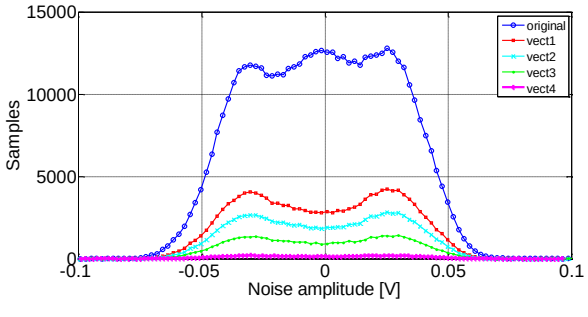


Figure IV-50 – Histogrammes des différents vecteurs temporels

b. Fréquence d'analyse

La fréquence d'échantillonnage du signal HF n'est pas vraiment importante à condition que cette fréquence soit supérieure à deux fois la fréquence de la porteuse du signal (critère d'échantillonnage de Shannon). Pour ce test, le signal HF est échantillonné et filtré de façon à récupérer des histogrammes pour différentes fréquences d'échantillonnage. La figure IV-51 permet d'observer ces différentes distributions de bruit. Comme on peut l'observer, l'amplitude de ces histogrammes peut être différente ; ce résultat est normal puisque le nombre d'échantillons augmente avec la fréquence d'échantillonnage. On obtient cependant des histogrammes de formes identiques pour toutes les fréquences d'échantillonnage. On en déduit que la fréquence d'échantillonnage n'a pas d'impact sur l'histogramme à condition qu'elle soit suffisamment grande par rapport à la fréquence de la porteuse du signal.

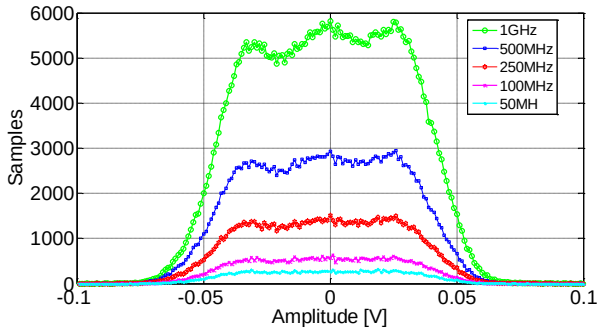


Figure IV-51 – Histogrammes obtenus pour différentes fréquences d'échantillonnage

C. Influence de la carte sur le lecteur (sans relais)

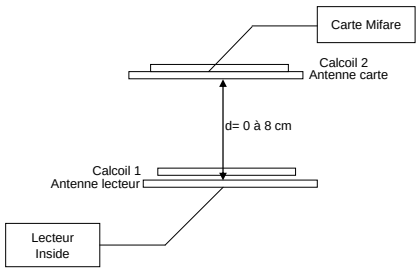


Figure IV-52 – Synoptique du système sans contact et du système de mesures

Pour cette expérience, nous étudions le bruit lorsqu'aucun relais n'est inséré entre le lecteur et la carte (figure IV-52). La carte est de type ISO14443-A et de marque NXP Mifare. Ce scénario est utilisé pour réaliser la phase de calibration de notre algorithme de détection. Les courbes obtenues durant cette expérimentation seront utilisées comme références et seront comparées avec les courbes obtenues durant une phase de communication. Même si le protocole n'est pas implémenté, on va pouvoir comparer les courbes obtenues dans les différents cas avec relais avec les courbes obtenues dans le cas sans relais.

a. Etude de la distance

Le couplage entre le lecteur et la carte, et donc la distance entre les deux antennes, ont une influence importante sur les histogrammes récupérés. Comme on peut le voir sur les figures IV-53 et IV-54 correspondant aux histogrammes enregistrés au niveau de la carte et au niveau du lecteur, la forme des histogrammes évolue avec la distance entre les deux antennes. Plus la distance augmente, et donc plus le couplage diminue, et plus l'influence de la carte au niveau du lecteur est faible. En effet, si on observe la figure IV-53, la largeur à mi-hauteur des histogrammes et donc la variance du bruit diminue lorsque la distance augmente au niveau du lecteur. Pour la figure IV-54, l'empreinte du bruit reste assez constante pour de faibles distances avec une forte influence du bruit de la carte et donc un histogramme large.

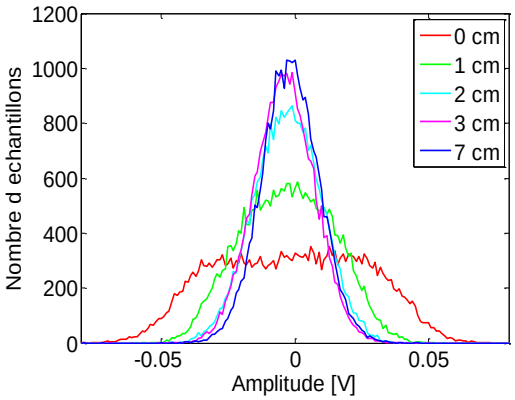


Figure IV-53 – Histogrammes obtenus au niveau du lecteur en fonction de la distance entre les antennes

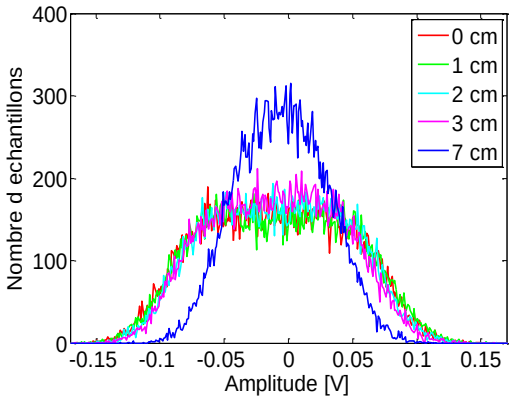


Figure IV-54 – Histogrammes obtenus au niveau de la carte en fonction de la distance entre les antennes

b. <u>Etude sur les standards</u>

Cette expérience a été réalisée pour déterminer l'impact de la norme sans contact utilisée sur le bruit récupéré. Pour que notre système soit le plus fiable possible, il serait intéressant que le bruit dépende de la norme utilisée pour obtenir une véritable empreinte de bruit. Nous utilisons donc trois normes sans contact : ISO 14443-A, ISO 14443-B et ISO 15693. Ces standards utilisent la même fréquence porteuse (13.56 MHz). Cependant, le codage, la durée d'un bit et le type de modulation ne sont pas les mêmes. La figure IV-55 présente les résultats de cette expérience. On observe d'importantes différences entre les histogrammes récupérés au niveau du lecteur. On en déduit donc qu'il serait possible de connaitre le standard utilisé par une carte juste en récupérant son histogramme.

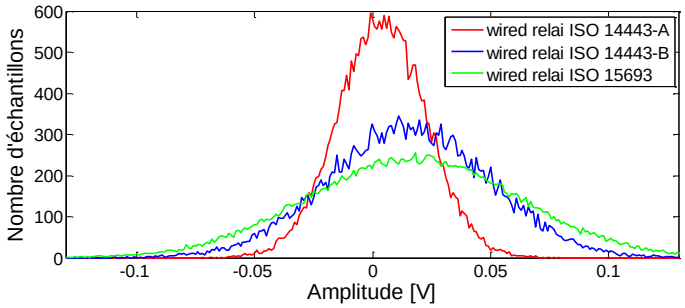


Figure IV-55 – Histogrammes obtenus au niveau du lecteur en fonction de la norme utilisée

c. <u>Etude sur les cartes d'un même standard</u>

Nous avons observé que la forme de l'histogramme dépendait de la norme sans contact utilisée. Cependant, il est nécessaire de vérifier s'il est possible de comparer différentes cartes utilisant le même standard. Pour cette expérimentation, les mesures ont été réalisées avec différentes cartes sans contact utilisant la norme sans contact ISO 14443-A. Le lecteur utilisé est le même pour quatre cartes différentes :

- Carte NXP Mifare
- Carte Oberthur IC ONE
- Carte SLB EASA MIFP
- Carte d'accès CEA

On extrait le bruit pour chacune de ces cartes. Les histogrammes de bruit correspondant à ces différentes cartes sont tracés sur la figure IV-56. Les résultats observés sont approximativement les mêmes pour les différentes cartes. Ainsi, il semble difficile de détecter l'empreinte d'une carte à partir du bruit récupéré au niveau du lecteur.

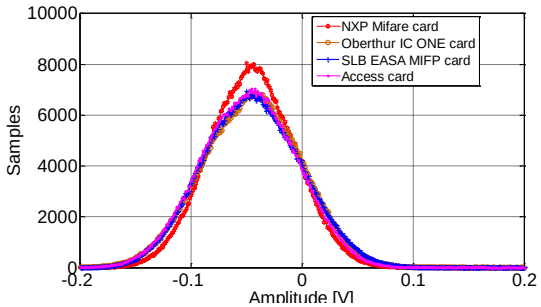


Figure IV-56 – Histogrammes obtenus au niveau du lecteur pour différentes cartes d'un même standard

D. Influence des différents types de relais

Dans cette partie, on compare les histogrammes de référence obtenus sans relais avec des histogrammes obtenus en présence de différents relais. Tous ces relais ont été étudiés dans la partie « Réalisation d'attaques ».

a. Relais filaire

Le premier relais étudié est le relais filaire ; c'est un relais de type « amplify and forward ». L'objectif de cette expérience est de prouver que cette attaque modifie le bruit au niveau du lecteur. On étudie donc les histogrammes obtenus au niveau de la bobine de calibration lecteur et on les compare avec ceux obtenus lors de l'étude sans relais. Nous avons montré dans la section « 2ème scenario: amplify and forward » qu'un relais de type « amplify and forward » introduisait plus de bruit qu'une communication directe entre un émetteur et un récepteur. Dans ce scénario, nous introduisons un relais filaire entre le lecteur et la carte et nous analysons l'histogramme obtenu pour différentes distances entre l'antenne lecteur et l'antenne A du relais. La figure IV-57 représente les histogrammes obtenus lors d'une communication directe entre le lecteur et la carte et ceux obtenus lors de l'ajout d'un relais. Tous ces histogrammes ont été obtenus pour différentes distances entre les antennes. Comme on peut l'observer sur la figure, le relais filaire introduit généralement plus de bruit que le système sans contact classique. Seuls les cas où la carte est proche du lecteur et qu'il y a une forte influence de celle-ci sur le lecteur introduisent un gain de bruit similaire aux cas avec le relais filaire. Il semble donc possible de détecter les relais filaires pour certaines distances. Cependant, il est difficile d'évaluer les histogrammes pour toutes les distances entre les antennes et il est donc possible de trouver des cas où le relais filaire possède un histogramme sensiblement identique à l'histogramme obtenu sans relais. Cela est vrai pour le paramètre distance, mais aussi pour la structure générale du relais filaire. En effet, il est impossible de tester toutes les possibilités de relais. De plus, il est possible qu'en augmentant la distance entre le lecteur et l'antenne A du relais que les histogrammes soient identiques avec et sans relais puisque l'antenne n'aura plus d'influence sur le lecteur (couplage trop faible).

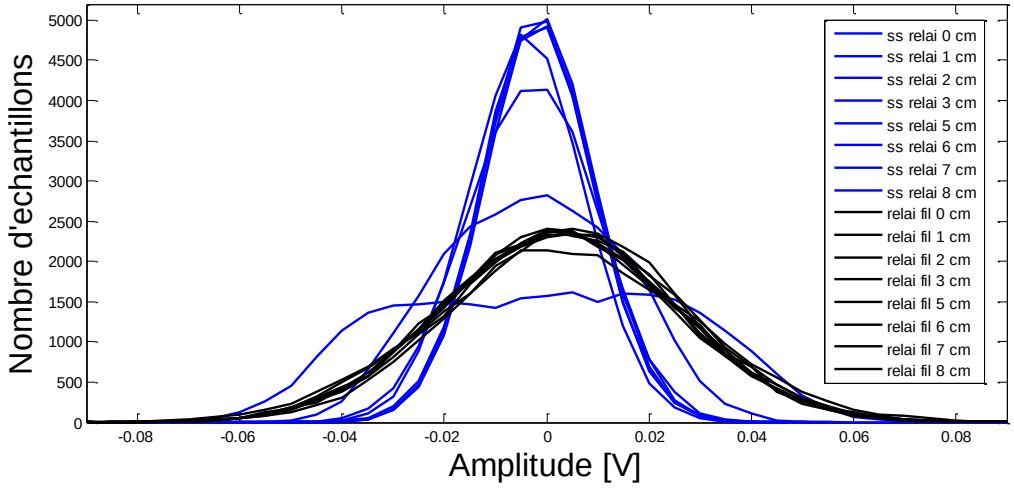


Figure IV-57 – Histogrammes obtenus au niveau du lecteur en fonction de la distance entre les antennes en présence d'un relais filaire

b. <u>Relais avec amplification</u>

Pour continuer de tester le relais « amplify and forward », on réalise des expériences sur un relais avec amplificateur de gain supérieur à 1. La figure IV-58 montre les histogrammes obtenus pour différentes distances dans le cas de relais « amplify and forward » et dans le cas sans relais. Ces résultats montrent l'influence du relais avec amplificateur sur le bruit mesuré au niveau du lecteur sans contact. Cependant, on observe cette différence uniquement pour certaines distances (distances faibles et donc forts couplages) donc il semble difficile de conclure de manière générale sur les résultats obtenus. Lorsque l'antenne A du relais est suffisamment éloignée du lecteur, les histogrammes obtenus avec et sans un relais sont identiques (courbes dont la largeur à mi-hauteur est la plus faible). Lorsque le couplage entre le lecteur et la carte est trop faible, il semble que ce relais n'ait plus d'influence au niveau du bruit du lecteur.

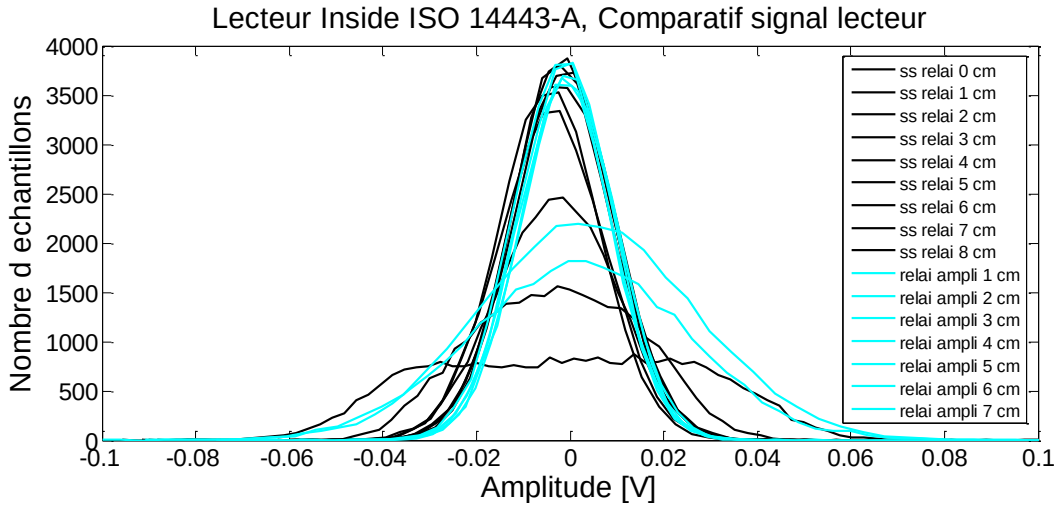


Figure IV-58 – Histogrammes obtenus au niveau du lecteur en fonction de la distance entre les antennes en présence d'un relais avec amplification

c. <u>Relais sans fil</u>

On réalise la même expérience avec le relais sans fil étudié dans la partie « Réalisation d'attaques ». La figure IV-59 montre la comparaison entre les signaux obtenus lors de l'attaque relais sans fil et les signaux obtenus lors d'une communication directe. On obtient des résultats

similaires aux résultats trouvés avec les autres relais. On observe bien une différence entre les deux types d'histogrammes, mais seulement pour certaines distances.

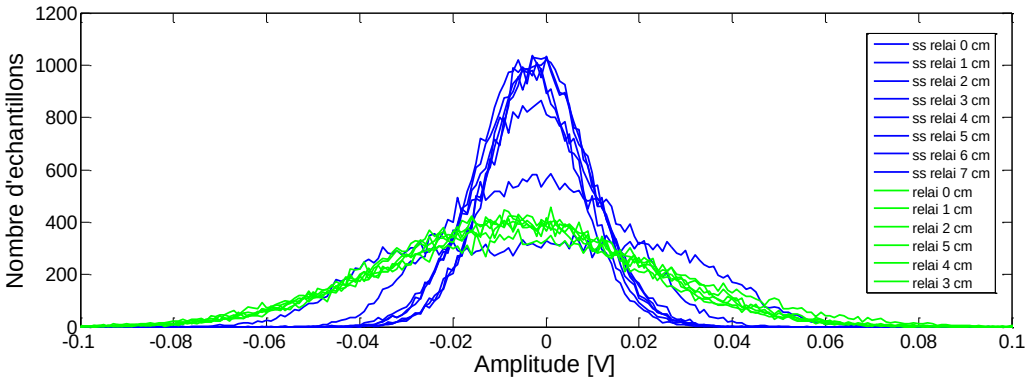


Figure IV-59 – Histogrammes obtenus au niveau du lecteur en fonction de la distance entre les antennes en présence d'un relais sans fil

E. Conclusion

Pour conclure sur cette campagne de mesures, nous avons montré qu'il était possible de détecter les relais de type « amplify and forward ». Cependant, il est difficile de dire si cette méthode fonctionne pour n'importe quel relais « amplify and forward » puisque l'on a vu que certaines distributions de bruit étaient très proches avec et sans relais. Il semble donc possible qu'un attaquant parvienne à réaliser l'attaque pour certaines distances entre le lecteur et la carte. Le meilleur compromis semble donc de réaliser plusieurs histogrammes lors de l'approche de la carte ou du relais de façon à conclure à partir d'histogrammes obtenus pour différentes distances entre le lecteur et la carte ou le relais.

5. Implémentation

A. Dispositif de test

La quantification du signal échantillonné par les oscilloscopes actuels est insuffisante. En effet, ce paramètre est souvent limité à 7 bits ce qui est relativement faible pour travailler sur un bruit modulé. Il est possible sur ces oscilloscopes d'augmenter cette résolution en moyennant le signal. Cependant, la moyenne agit alors comme un filtre et perturbe notre analyse du bruit.

Cette limite est l'un des paramètres qui nous a poussé à utiliser le lecteur Lrfv7 (dont nous avons parlé dans plusieurs chapitres) pour développer et implémenter notre solution de façon à utiliser le convertisseur analogique-numérique 10 bits de cette carte d'expérimentation. Son système d'échantillonnage est la base de notre solution et va nous permettre de récupérer les échantillons de notre signal. L'échantillonnage sur les extremums de la sous-porteuse permet de récupérer l'enveloppe du signal et donc le bruit ; l'analyse du bruit est donc basée sur la bande fréquentielle proche du 13.56 MHz (fréquence de la porteuse du signal). L'avantage de cette implémentation est donc de récupérer 3 bits de précision supplémentaires par rapport aux oscilloscopes. On perd cependant cet avantage par une fréquence d'échantillonnage très inférieure (de plusieurs GHz à 27.12 MHz).

Le signal récupéré est malheureusement détérioré par l'ensemble de la chaine de réception analogique de la carte électronique. Le filtre analogique de réception de la carte Lrfv7 coupe les fréquences en dehors de la bande du 13.56 MHz.

Deux autres systèmes de la chaine de réception sont à prendre en compte (figure IV-60). Tout d'abord, un amplificateur à gain variable contrôlé par le FPGA est intégré à la carte pour obtenir une résolution maximale sur le convertisseur analogique numérique. L'amplitude crête à crête du

signal en sortie de la chaine d'amplification est donc toujours proche de 1.2 V (la dynamique de notre ADC). Ce gain variable influe sur l'amplitude de notre bruit. Il sera donc nécessaire de récupérer la valeur de cette amplification et de l'utiliser lors de l'analyse statistique pour retrouver l'amplitude du bruit avant amplification.

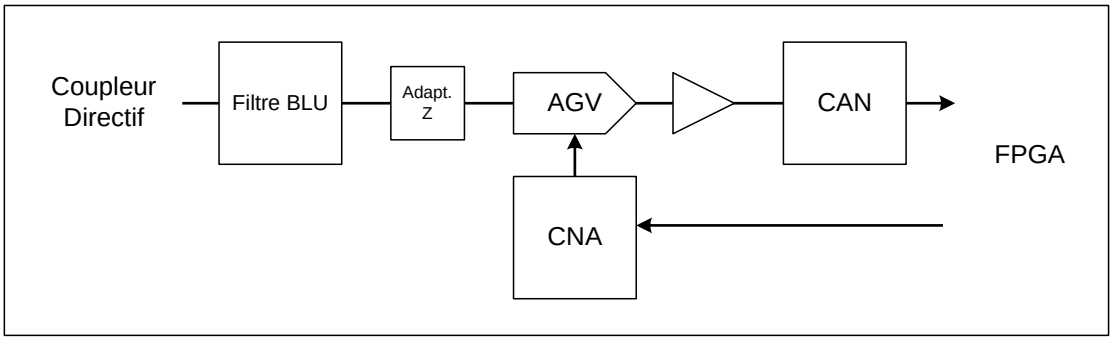


Figure IV-60 – Synoptique de la chaine de réception de Lrfv7

Un autre élément de notre chaine de réception est le convertisseur de données qui échantillonne le signal à 27.12 MHz. Le signal est donc échantillonné dans le meilleur cas sur les extremums positifs et négatifs du signal. Dans la réalité, l'horloge d'échantillonnage (malgré l'algorithme de recherche de maximum) peut être légèrement décalée. Le décalage maximal possible est la moitié de la période de la fréquence de travail de notre FPGA qui est de 108.48 MHz, le signal peut donc être échantillonné à 5 ns avant ou après l'extremum. Comme on peut le voir sur la figure IV-61, ce décalage introduit une modification maximale de l'amplitude de 12 % de la valeur maximale. Bien que l'on perde en précision, on garde cette imprécision pendant toute la durée de la mesure ; tous les échantillons récupérés sont donc valides pour une même mesure, mais un décalage maximal de 12 % est possible entre deux mesures.

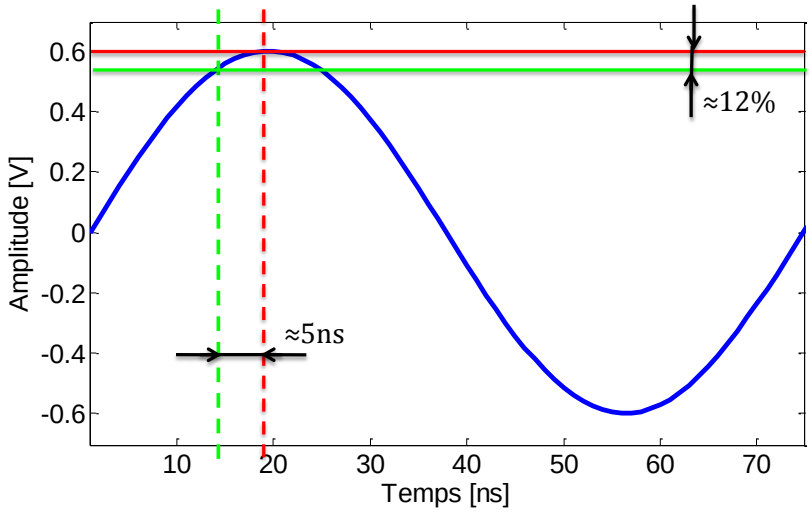


Figure IV-61 – Précision de l'échantillonnage sur Lrfv7

Si l'on compare cette résolution avec celle de l'oscilloscope dont la résolution est de 7 bits (128 valeurs) pour un signal proche des 1.2 Vcc, on obtient une incertitude de moins de 1% entre deux mesures.

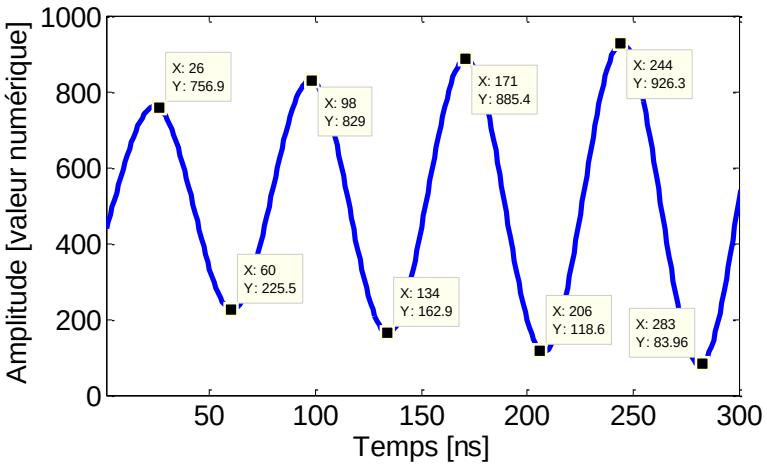
L'architecture VHDL développée est assez simple ; elle permet essentiellement d'échantillonner le signal, de créer l'histogramme et d'envoyer ces données vers le microcontrôleur NIOS via un bus SPI. L'interface logicielle permet alors de récupérer les différents échantillons qui seront analysés sous Matlab.

La calibration de l'échantillonnage se fait en deux phases :

- Dans un premier temps, le lecteur sans contact optimise la valeur du gain de la CAG de façon à utiliser toute la dynamique de l'ADC sans saturer. En fonction de la valeur de l'amplitude des échantillons récupérés en sortie de l'ADC, la structure VHDL modifie la valeur d'une résistance numérique agissant directement sur la valeur du gain de l'amplificateur via un port SPI.
- Dans un second temps, le lecteur sans contact réalise une recherche de maximum de façon à échantillonner le signal reçu sur les extremums de la porteuse. La fréquence de la porteuse (13.56 MHz) et la fréquence d'échantillonnage (27.12 MHz) sont générées à partir de la même fréquence (108.48 MHz) utilisée pour toute l'architecture VHDL. Ainsi, il n'existe aucun glissement fréquentiel au niveau de l'échantillonnage et donc on peut numériser périodiquement le signal. La recherche de maximum s'effectue en vérifiant l'amplitude des échantillons lors d'un glissement de la fréquence d'échantillonnage à 108.48 MHz (une fois le gain fixé). Pour cette fréquence, il est possible de décaler le signal avec une précision de la période du 108.48 MHz.

L'histogramme d'un signal est juste la mise en tableau des échantillons en fonction de leurs valeurs. La résolution de notre convertisseur est de 10 bits : les valeurs des échantillons sont donc comprises entre 0 et 1023. On crée donc une structure de 1024 vecteurs. Dans chacun de ces vecteurs, on va incrémenter le nombre d'éléments dont l'amplitude est l'indice du vecteur. Par exemple, si l'échantillon i possède une amplitude de 902, on va incrémenter de 1 le vecteur n°902.

La figure IV-62 montre la création de cet histogramme basé sur la valeur de l'amplitude numérique de notre signal.



Amplitude	Nombre d'échantillons
0	X_0
…	
84	X_{84} +1
…	
118	X_{118} +1
…	
163	X_{163} +1
…	
225	X_{225} +1
…	
757	X_{757} +1
…	
829	X_{829} +1
…	
885	X_{885} +1
…	
926	X_{926} +1
…	
1023	X_{1023}

Figure IV-62 – Récupération des échantillons sur les extremums du signal et création de l'histogramme

Cette structure de 1024 vecteurs est envoyée au processeur NIOS intégré au FPGA via une liaison SPI. Il est alors possible de récupérer ces données sur un ordinateur en utilisant directement le logiciel pilotant le processeur ou en développant un GUI.

Nous cherchons uniquement à observer les variations du bruit dans le champ du lecteur en présence d'une carte ou d'un relais. Nous n'avons pas jugé nécessaire de faire ces

expérimentations lors d'une modulation de la carte ou du lecteur. Aucune requête n'est donc envoyée par le lecteur ou la carte.

Le signal obtenu est un histogramme centré sur une valeur proche de 511 (la moyenne numérique de notre signal) et possédant deux franges dont les valeurs correspondent à l'enveloppe du signal. En effet, l'échantillonnage à 27.12 MHz nous permet de récupérer uniquement les extremums du signal. La moyenne de chacune de ces franges est l'amplitude moyenne du signal et la base est la variation des maximums ou des minimums de l'enveloppe de la porteuse. La figure IV-63 est un exemple d'histogramme obtenu lorsqu'une carte était présente à côté du lecteur. On en déduit une valeur moyenne proche de 136 pour les minimums et de 894 pour les maximums.

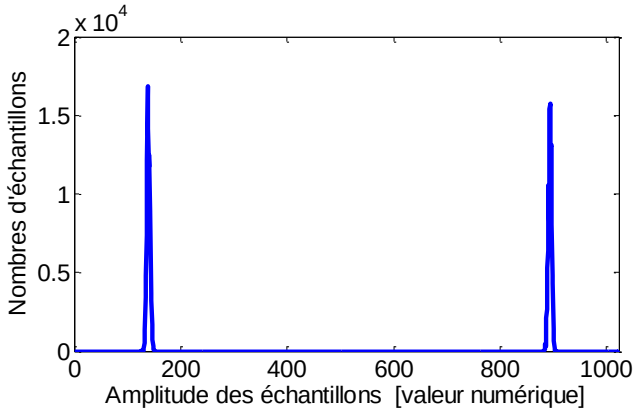


Figure IV-63 – Exemple d'histogrammes obtenu

Comme nous l'avons dit auparavant, l'histogramme est un ensemble de 1024 vecteurs de bits numérotés de 0 à 1023. On a ajouté un 1025ème vecteur correspondant à la valeur du potentiomètre numérique utilisé pour la CAG. Cette donnée servira pour normaliser nos différents histogrammes. Chaque histogramme est basé sur un enregistrement de 225000 échantillons soit une durée d'analyse de 8.3 ms. Les histogrammes récupérés sont alors analysés à l'aide du logiciel Matlab de façon à récupérer toutes les informations nous permettant de caractériser la présence d'un relais.

Soit xi ∈ [0 ; 1023] la valeur de l'amplitude de l'échantillon et ni le nombre d'échantillons dont l'amplitude est xi, il est alors possible de calculer la probabilité p(xi) d'obtenir la valeur xi :

$$p(x_i) = \frac{n_i}{\sum_{i=0}^{i=1023} n_i} \quad \text{(IV-17)}$$

Il est alors possible de calculer la moyenne E[xi] de l'amplitude du signal pour recentrer parfaitement notre signal en soustrayant la moyenne du pic de droite $E[x_{i2}]$ à la moyenne du pic de gauche $E[x_{i1}]$. Pour j ∈ [1 ; 2], on a :

$$E[x_{ij}] = \sum_{i=0}^{i=1023} p(x_{ij}) * x_{ij} \quad \text{(IV-18)}$$

Il est nécessaire de normaliser la valeur de ce centre en utilisant la valeur du gain G :

$$E[x_{ij}]_{norm} = \frac{E[x_{i2}] - E[x_{i1}]}{G} \quad \text{(IV-19)}$$

De la même façon, on normalise les nouvelles valeurs de l'amplitude xic par la valeur du gain (une fois l'histogramme centré en zéro) :

$$x_{ic\_norm} = \frac{x_i - E[x_{ij}]_{norm}}{G} \quad \text{(IV-20)}$$

Pour faciliter l'extraction des données, on ne conserve qu'un seul pic. On ne s'intéresse donc qu'aux données négatives ou positives. On peut alors calculer la variance de ce pic à partir de ces valeurs d'amplitude xic_normplus :

$$variance = \sum x_{ic_{normplus}} * p(x_{ic_{normplus}}) \quad \text{(IV-21)}$$

A partir de cette analyse, il est possible de tracer pour un système donné le courant, le gain et la variance en fonction de la distance, mais aussi la variance en fonction du courant. Ces informations permettent de quantifier le bruit au niveau de l'émetteur et devrait permettre de détecter un relais de type « amplify and forward ». Pour comparer les différents relais entre eux et le système sans contact, il est nécessaire d'avoir une référence commune entre les différents scénarios. Pour un courant identique à chacun de nos scénarios, on va observer si la quantité de bruit diffère. Si elle n'évolue pas ou très peu, on peut conclure que l'apport du bruit n'est pas suffisant pour que notre système soit susceptible de le détecter.

B. Système sans relais

Pour cette première expérience qui nous servira de référence, on a pour objectif de mesurer les paramètres de bruit lorsqu'aucun relais n'est présent entre le lecteur et la carte. Comme on peut le constater sur la figure IV-64, le seul paramètre variant au cours de l'expérience est la distance entre le lecteur et la carte. La figure IV-65 permet d'observer l'histogramme obtenu pour certaines de ces distances et pour des valeurs positives. Comme on peut l'observer, la distance a un impact sur la distribution de bruit (largeur de l'histogramme) mais aussi sur l'amplitude du signal (les histogrammes ne sont pas centrés autour de la même amplitude).

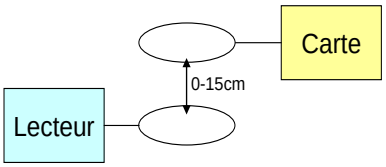


Figure IV-64 – Système d'analyse

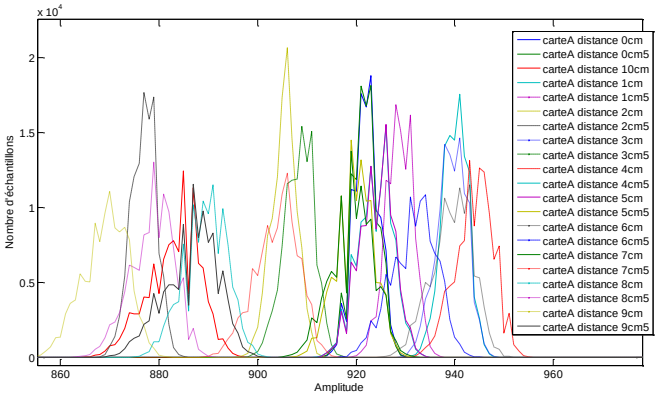


Figure IV-65 – Histogrammes obtenus sur les échantillons positifs

Nous avons travaillé sur les normes ISO14443-A et ISO14443-B. A partir des différents histogrammes obtenus et de la valeur du gain utilisée par la CAG, il est possible de tracer différentes courbes. La figure IV-66 montre une image du courant dans la chaine de réception (amplitude des échantillons) et le gain de la CAG pour les différentes distances entre le lecteur et 2 cartes sans contact différentes. Le courant est fonction de l'influence de la carte puisque le coupleur au début de la chaine de réception permet de mesurer la désadaptation de l'antenne lecteur introduite par la carte.

Le calcul de la variance des différents histogrammes permet de tracer la fonction variance en fonction du courant dans l'antenne (figure IV-67). Le courant dans l'antenne décroit avec l'augmentation de la distance. Ce résultat est correct puisque l'influence de la carte diminue. On observe alors que plus le courant est important et plus la variance (et donc la quantité de bruit) est importante. Si l'on compare ce résultat avec les premiers résultats expérimentaux, on remarque que l'on obtient une conclusion totalement différente et illogique puisque le bruit

semble diminuer lorsque la carte se rapproche. Cette méthode ne semble donc pas fiable pour mesurer le bruit.

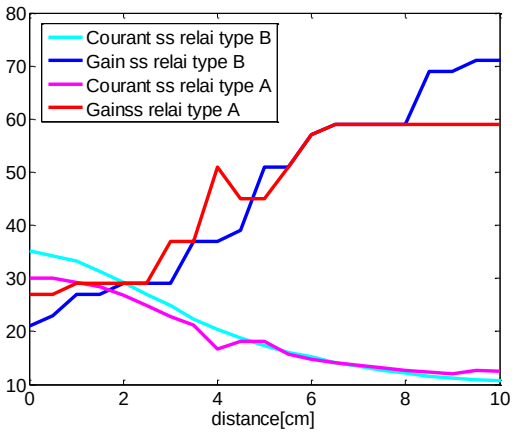


Figure IV-66 – Comparaison du courant et du gain obtenus pour deux standards de cartes sans contact différents

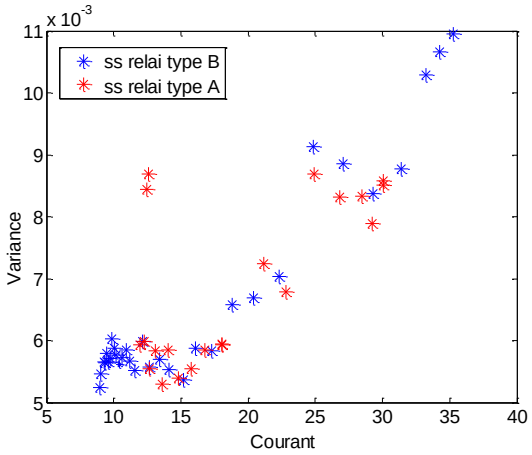


Figure IV-67 – Comparaison de la variance en fonction du courant pour deux standards de cartes sans contact différents

C. Système avec relais

a. Relais filaire

On étudie l'impact d'un relais filaire sur les échantillons récupérés au niveau du lecteur ainsi que la variance calculée. On étudie différents scénarios comme le montre les figures IV-68, IV-69 et IV-70. Ces différents scénarios utilisent différentes antennes et vont permettre de donner différentes conclusions : l'impact de l'antenne relais au niveau du lecteur et de la carte sur le bruit.

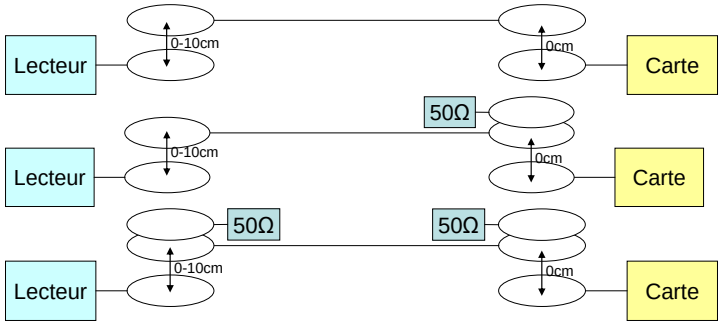


Figure IV-68 – Scénario 1 : antenne du relais => antennes ID1

Figure IV-69 – Scénario 1 : antenne du relais => antenne ID1 et antenne marguerite

Figure IV-70 – Scénario 1 : antenne du relais => antennes marguerites

Les figures IV-71 et IV-72 permettent d'observer différents résultats. Tout d'abord, on remarque que les deux relais utilisant une antenne ID1 au niveau de l'antenne relais proche du lecteur possèdent la même forme de courant et gain. Cependant, le relais utilisant deux antennes marguerites possède une courbe de courant complètement différente. Cette étude permet de montrer que l'antenne relais proche de la carte n'a pas une forte influence sur le courant au niveau du lecteur, mais aussi que chaque antenne a une influence sur l'antenne du lecteur. Cette influence peut être utilisée comme empreinte à condition de connaître les histogrammes d'une antenne donnée pour toutes les distances.

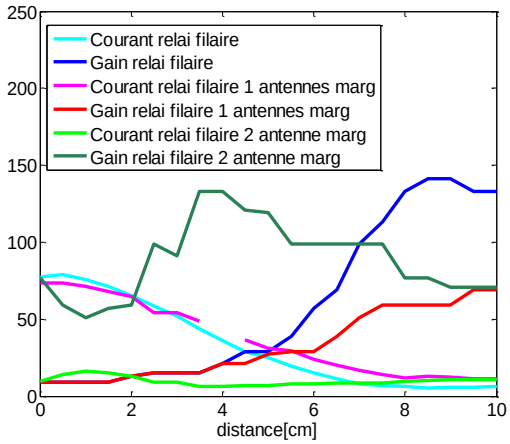


Figure IV-71 – Comparaison du courant et du gain obtenus pour différents scénarios de relais filaire

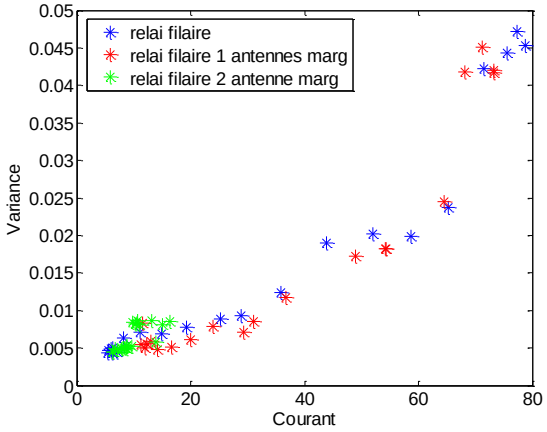


Figure IV-72 – Comparaison de la variance en fonction du courant pour différents scénarios de relais filaire

b. Comparaison de tous les relais

L'objectif est de montrer si le relais possède une influence sur la variance du bruit récupéré au niveau du lecteur. Nous avons donc analysé les différents histogrammes obtenus pour les différents relais étudiés dans le chapitre « Réalisation d'attaques ». Les résultats montrés sur la figure IV-73 sont décevants puisque pour un même courant, on n'observe pas de différences notables au niveau de la variance. Il n'est donc pas possible de conclure sur la présence d'un relais avec un unique histogramme comparé à l'histogramme de référence.

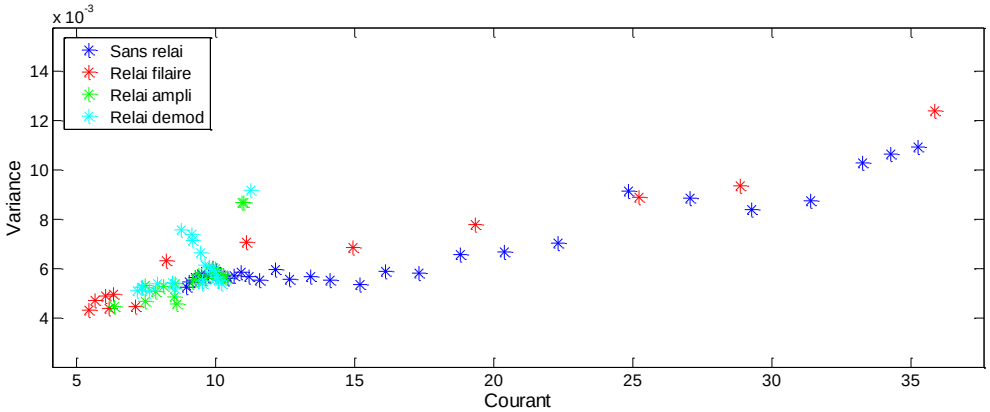


Figure IV-73 – Comparaison de la variance en fonction du courant pour les différents relais

D. Authentification d'antennes

Nous avons cependant observé qu'il était possible de trouver une empreinte pour chaque antenne différente. Nous allons donc vérifier si cette observation se révèle vrai avec quatre antennes différentes au niveau de la carte. Les antennes utilisées sont :

- Une carte sans contact classique
- Une antenne marguerite
- Une antenne double-huit
- Une antenne ID1

Toutes ces antennes sont répertoriées et leurs fonctionnements expliqués dans les annexes. On observe bien une différence dans le comportement de ces différentes antennes (figures IV-74

et IV-75). On remarque que pour les antennes double-huit et marguerites, la carte a la même influence sur le lecteur quelle que soit la distance entre les deux.

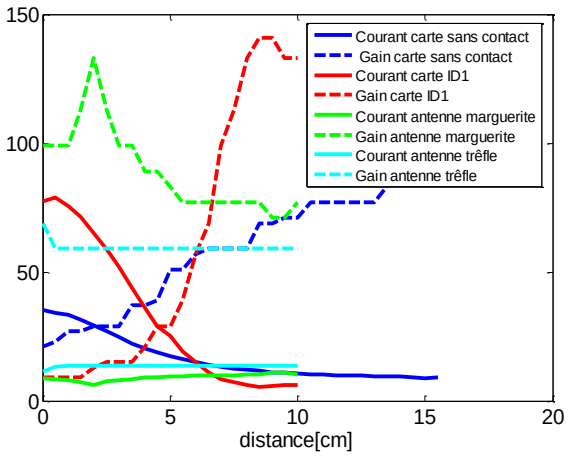


Figure IV-74 – Comparaison du courant et du gain obtenus pour différentes antennes de relais

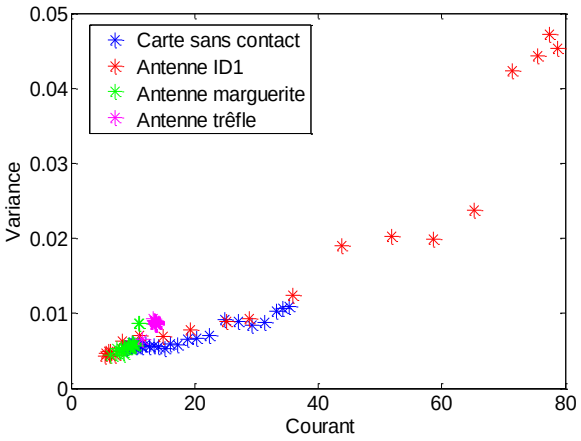


Figure IV-75 – Comparaison de la variance en fonction du courant pour différentes antennes de relais

E. Conclusion

Nous avons implémenté notre solution sur un système sans contact de métrologie. Les résultats sont décevants puisque le bruit ne nous permet pas de détecter la présence d'un relais. On a cependant remarqué que le courant dans la chaîne de réception pouvait permettre de vérifier la présence d'une antenne en particulier. Il existe alors deux solutions pour parvenir à identifier un relais ou un type d'antennes :

- Une première solution consiste à étudier l'approche de la carte ou du relais de façon à avoir plusieurs histogrammes à différentes distances.
- Une autre solution consiste à connaître la distance à laquelle est placée l'antenne lors du test.

Dans les deux cas, on utilise un paramètre pour conclure sur le dispositif sans contact à proximité du lecteur.

6. Avantages de cette solution et travaux futurs

A. Avantages

Nous avons montré la difficulté d'utiliser une solution basée sur le bruit, en particulier sur les systèmes sans contact. Cependant, une telle solution apporte de nombreux avantages au niveau sécurité et implémentation. Tout d'abord, cette contre-mesure peut s'ajuster à n'importe quelles technologies sans fil (RFID, réseaux de capteurs, réseaux véhiculaires) et pour la plupart des applications (militaire, surveillance, authentification,…).

Cette solution est théoriquement fiable au niveau sécurité puisqu'elle utilise la couche physique du système sans contact ou sans fil. Il est ainsi difficile pour l'attaquant de réaliser une empreinte physique de bruit qui puisse ressembler à l'empreinte de référence. L'utilisation de protocoles cryptographiques n'est alors pas nécessaire et notre solution est indépendante des protocoles haut niveau. La modification des normes existantes n'est pas utile.

Contrairement aux solutions existantes, notre solution ne nécessite aucun ajout technologique. L'utilisation de type d'antennes spécifiques ou d'horloges synchronisées n'est pas nécessaire. Le coût d'une telle solution est donc relativement faible.

B. Travaux futurs

L'étude nécessite encore beaucoup de travail pour arriver à une conclusion sur une possible utilisation de cette solution dans le domaine du sans contact. La non-linéarité du canal introduit par le couplage magnétique est particulièrement complexe. Le couplage entre les deux éléments a un fort impact sur le bruit récupéré par le lecteur et aussi l'amplitude du signal. Une nouvelle étude théorique doit être réalisée pour interpréter la non-linéarité du canal et savoir si la solution peut être ajustée pour un système sans contact. A partir de cette étude, de nouvelles expérimentations devront être réalisées pour analyser des signaux expérimentaux..

A partir de l'implémentation réalisée, un protocole de comparaison d'histogrammes doit permettre de comparer le ou les histogrammes de référence avec les histogrammes obtenus lors de la recherche de détection de relais.

Une autre solution est la détection de relais en réalisant une cartographie de l'approche carte. Il est possible d'implémenter une solution basée sur un histogramme glissant. C'est-à-dire qu'on accumule dans une FIFO des échantillons au fur et à mesure. Ces échantillons permettent de réaliser différents histogrammes et de visionner l'approche de la carte ou de l'antenne relais. Cette cartographie facilite la détection du relais car on connait ainsi le comportement des échantillons en fonction du couplage entre l'antenne lecteur et l'antenne carte ou relais.

7. Conclusion

Il est très difficile de donner des conclusions sur ce travail concernant le bruit, notamment sur la fiabilité d'une solution utilisant le bruit. Cette étude portait sur une contre-mesure permettant la détection d'attaques relais dans les communications sans fil et sans contact. Cette solution reposait sur les caractéristiques du canal sans fil. Il a été démontré qu'une solution basée sur l'analyse du bruit au niveau de l'émetteur ou du récepteur permettait de détecter un relais. En effet, l'ajout d'un relais de type « amplify and forward » entre l'émetteur et le récepteur ajoute un bruit mesurable. Cependant, les différentes expérimentations réalisées sur des systèmes sans contact n'ont pas donné les résultats escomptés. Bien que l'on retrouve des différences au niveau de l'amplitude de bruit pour certaines distances entre le lecteur et la carte ou relais, il est impossible de conclure que notre solution fonctionne pour n'importe quels relais et distance. De la même façon, l'implémentation de cette solution sur un lecteur sans contact ne permet pas d'identifier la présence d'un relais, mais peut permettre d'authentifier une antenne par ces caractéristiques. Le système sans contact n'est pas idéal pour tester une solution sur le bruit car le canal utilisé n'est pas linéaire (il dépend du couplage entre le lecteur et la carte) contrairement au canal utilisé par les systèmes sans fil. Nos expérimentations ne prouvent donc pas que la solution ne fonctionne pas pour les systèmes sans fil. Pour les systèmes sans contact, il est possible de caractériser la communication (avec ou sans relais) en réalisant une cartographie du bruit et de l'amplitude du signal lors de l'approche de la carte par l'utilisateur ou en possédant une information de couplage ou de distance entre le lecteur et la carte.

Chapitre V. Le lecteur bruité

1. Introduction du chapitre

L'eavesdropping est une attaque potentiellement dangereuse puisqu'elle permet à un attaquant de récupérer des informations confidentielles échangées entre un lecteur et une carte en mesurant le champ radiofréquence émis par le lecteur. Son développement et son implémentation sont assez simples puisqu'une antenne reliée à un oscilloscope peut permettre de collecter les données binaires échangées. Alors que la distance de communication entre un lecteur et une carte est proche de la dizaine de centimètres, un espion est capable de récupérer le signal envoyé par un lecteur à plus de 20 mètres (200 fois la distance de fonctionnement). En raison du type de modulation utilisée, le signal de la carte est plus difficile à espionner ; la distance obtenue est d'environ 4 mètres (soit 40 fois la distance de fonctionnement). Pour améliorer la sécurité des données confidentielles contenues dans la mémoire de la carte, il est nécessaire de sécuriser les échanges de la carte vers le lecteur. Le lecteur bruité a été développé en 2007 par une équipe du CEA Léti. L'objectif de ce système, introduit dans l'état de l'art, est de bruiter le canal sans contact. Ainsi, le lecteur peut dissimuler les trames échangées avec une carte et éviter ainsi tout espionnage de la communication par un attaquant. Le lecteur active un bruit analogique et aléatoire lorsque la carte envoie des informations confidentielles. Connaissant le bruit envoyé, le lecteur est capable de retrouver le signal de la carte.

Durant cette thèse, nous avions pour objectif de réaliser plusieurs améliorations concernant le lecteur bruité. Tout d'abord, il est intéressant d'étudier le remplacement de l'antenne marguerite par une antenne conforme à la norme ISO10373 pour simplifier le système actuel. Ensuite, le choix du gain de l'amplification du bruit est actuellement manuel, l'idéal serait de trouver une solution permettant d'optimiser la valeur du gain en fonction de la distance entre les antennes lecteur et cartes. Actuellement, le lecteur ne permet pas de bruiter n'importe quel protocole de communication, une analyse du bruit sera réalisée pour identifier les bruits à générer pour les différentes normes sans contact. D'autres améliorations sont étudiées dans cette partie.

Même si la plupart des idées ont été mises en place, nous montrerons les difficultés rencontrées et la démarche scientifique utilisée pour identifier des solutions.

2. Etat de l'art

Dans cette partie consacrée à l'état de l'art, nous allons nous intéresser aux différentes normes sans contact et au lecteur bruité actuel. Cette étude permettra de montrer les différentes faiblesses de cette contre-mesure et des moyens à mettre en œuvre pour l'améliorer.

A. Les normes

Pour comprendre toutes les spécificités du lecteur bruité existant et des développements réalisés dans ce chapitre, il est important de rappeler certaines caractéristiques des normes ISO 14443 type A et B) et de la norme ISO15693. La norme ISO14443 est principalement utilisée pour l'identification de personnes tandis que la norme ISO15693 est utilisée pour l'identification d'objets. Nous introduirons les parties 2 et 3 de ces normes, c'est-à-dire celles dédiées à la couche physique des systèmes sans contact.

a. Premières caractéristiques

La fréquence porteuse imposée pour ces différentes normes est le 13.56 MHz avec une précision de plus ou moins 7 kHz. Dans la norme ISO14443, la puissance du champ RF au niveau du récepteur doit être comprise entre 1.5 et 7.5 A/m pour que celui-ci soit opérationnel. Pour la norme ISO15693, le récepteur possède moins de ressources de calculs et nécessite moins d'énergie pour fonctionner. Le champ magnétique nécessaire au fonctionnement d'un tel transpondeur doit donc être compris entre 0.150 et 5 A/m. La distance de communication est donc bien plus élevée pour les dispositifs utilisant cette norme.

Dans le cas de la norme ISO14443 (type A et type B), le débit sera 106kbits/s (1 symbole dure 9.44 µs). Pour la norme ISO15693, le codage avec une unique sous-porteuse sera étudié avec un débit de 26.48kbits/s.

b. Modulation et codage

Le lecteur bruité brouille uniquement la communication de la carte vers le lecteur. Nous nous intéressons donc uniquement au codage et à la modulation utilisés par la carte sans contact pour transmettre des données au lecteur. En effet, la connaissance des caractéristiques du signal à brouiller est indispensable pour générer le bruit le plus adapté mais aussi pour synchroniser le signal de la carte avec le bruit. Tous les récepteurs que nous présentons ici transmettent des données en utilisant la modulation de charge. Les transpondeurs modulent la charge aux bornes de leurs antennes ; le résultat est une modification du champ radiofréquence et du courant dans l'antenne du lecteur.

Dans la norme ISO14443-A (figure V.3):

- La fréquence sous-porteuse est égale à fc/16, soit environ 847 kHz
- Modulation de la sous-porteuse: OOK (On-Off Keying)
- Codage de la sous-porteuse: Manchester

La valeur logique '1' est représentée par une modulation de la porteuse pendant la première moitié de la période du symbole (4.72 µs) (figure V.1). La seconde moitié du symbole n'est pas modulée.

La valeur logique '0' est représentée par une modulation de la porteuse pendant la seconde moitié de la période du symbole (4.72 µs) (figure V.2). La première moitié du symbole n'est pas modulée.

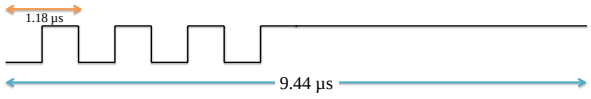


Figure V.1 – Codage ISO14443-A : '1' logique

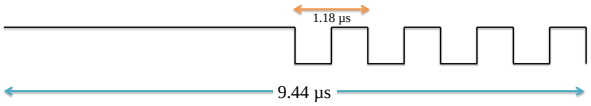


Figure V.2 – Codage ISO14443-A : '0' logique

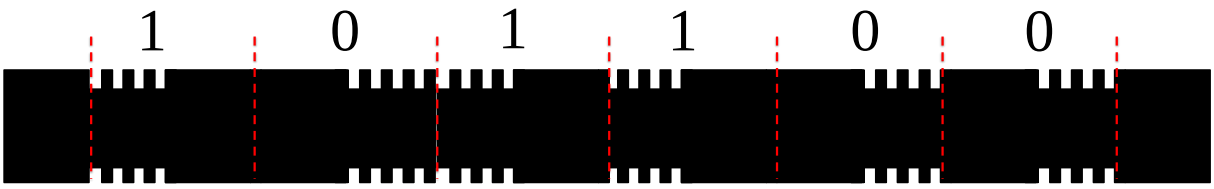


Figure V.3 – Codage et modulation ISO14443-A (Modulation : OOK ; codage : manchester)

Dans la norme ISO14443-B (figure V.6):

- La fréquence sous-porteuse est égale à fc/16, soit environ 847 kHz
- Modulation de la sous-porteuse: BPSK
- Codage de la sous-porteuse: NRZ-L

La différence entre les deux valeurs logiques '0' et '1' est caractérisée par une variation de phase de 180° de la fréquence sous porteuse (figure V.4 et V.5). Avant la réponse de la carte, cette dernière module le champ magnétique, l'état de phase de cette modulation correspond à une valeur logique '1'.

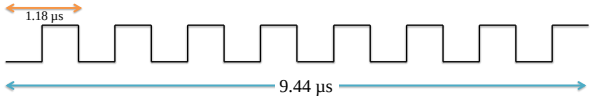


Figure V.4 – Codage ISO14443-B: '1' logique

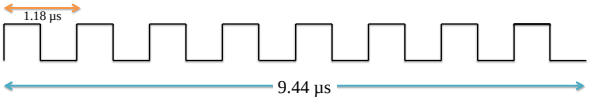


Figure V.5 – Codage ISO14443-B: '0' logique

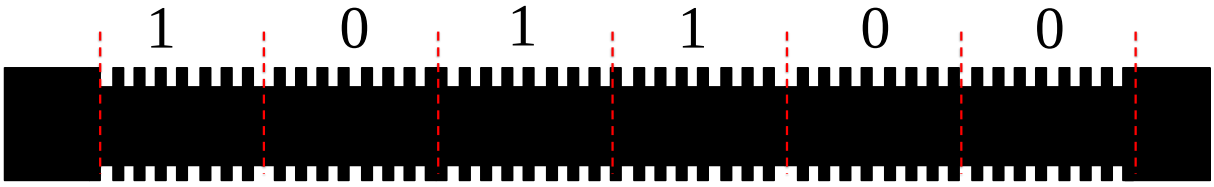


Figure V.6 – Codage et modulation ISO14443-B (Modulation : BPSK ; codage : NRZ-L)

Dans la norme ISO15693 (figure V.9):

- La fréquence sous-porteuse est égale à fc/32, soit 423.75 kHz
- Modulation de la sous porteuse: OOK
- Codage de la sous porteuse: Manchester

La valeur logique '0' est représentée par une modulation de la porteuse pendant la première moitié de la période du symbole (18.88 µs) (figure V.8). La seconde moitié du symbole n'est pas modulée.

La valeur logique '1' est représentée par une modulation de la porteuse pendant la seconde moitié de la période du symbole (18.88 µs) (figure V.7). La première moitié du symbole n'est pas modulée.

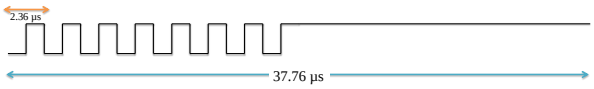


Figure V.7 – Codage ISO15693: '0' logique

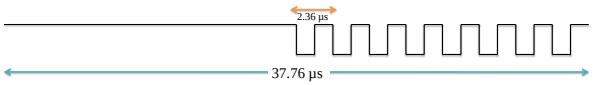


Figure V.8 – Codage ISO15693: '1' logique

Figure V.9 – Codage et modulation ISO15693 (Modulation : OOK ; codage : manchester)

c. <u>Format des trames</u>

L'étape de synchronisation du bruit avec le signal provenant de la carte est très importante. Pour identifier les possibilités de synchronisation, il est nécessaire d'étudier la réponse de la carte, et particulièrement le début de cette réponse et de la modulation de charge.

Dans la norme ISO14443-A, le début de la trame (SOF : Start of Frame) est identique à une valeur logique '1' (figure V.10). Le transpondeur module sa charge pendant la première moitié du temps symbole.

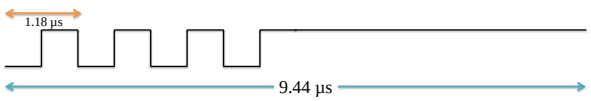


Figure V.10 – Début de trame ISO14443-A

Dans la norme ISO14443-B, le début de la trame est découpé en deux phases (figure V.11). Le transpondeur module sa charge pendant la première partie du SOF pour que le lecteur identifie la phase du signal. Ainsi, ce dernier pourra reconnaitre la valeur logique du bit en utilisant la phase de référence qui correspond à la valeur logique '1'. Cette première partie dure entre 10 et 11 durées symboles (94.4 à 103.84 µs). La deuxième partie est réalisée après un changement rapide de la phase de la sous-porteuse. La carte envoie 2 à 3 symboles '0' pour une durée de 18.88 à 28.32 µs.

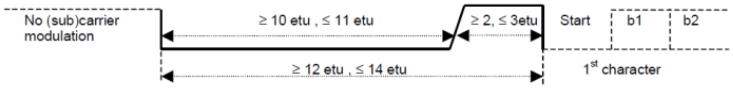


Figure V.11 – Début de trame ISO14443-B

Le début de trame de la norme ISO15693 est divisé en trois parties (figure V.12) :

- Une partie non modulée de durée 56.64 µs
- Une partie consistant en 24 alternances de sous porteuse à 423.75 kHz (durée = 56.64 µs)
- La troisième partie correspondant à une valeur logique '1'

Figure V.12 – Début de trame ISO15693

B. Le lecteur bruité actuel

Le principe de base du lecteur bruité repose sur le mode de communication des systèmes sans contact. En effet, l'utilisation du couplage inductif pour transmettre les données n'autorise pas le mode de communication full-duplex. Le lecteur module son champ radiofréquence pour transmettre des informations. Le lecteur continue d'activer ce champ RF pour alimenter la carte sans contact. La carte peut moduler le signal RF du lecteur en commutant la charge résistive (ou capacitive) aux bornes de son antenne. Cette modification de la charge équivalente de la carte altère le couplage entre les antennes de façon synchrone avec l'horloge du lecteur. Les variations du champ électromagnétique au niveau du lecteur sont perçues comme la transmission de données de la carte vers le lecteur.

Le lecteur bruité est un lecteur sans contact modifié permettant l'envoi simultané d'un bruit analogique et du signal RF du lecteur lors de la réponse de la carte. La carte reste opérationnelle malgré l'ajout de bruit dans le champ RF permettant de l'alimenter. Elle peut envoyer des données sur ce canal bruité en évitant ainsi tout espionnage de la communication par un attaquant potentiel. En effet, une sonde de champ ou toute autre antenne inductive ne reçoit qu'un message brouillé ; elle ne peut dissocier les données du bruit. Sachant que le lecteur connait le bruit qu'il a émis, il est capable de le soustraire au signal reçu de façon à récupérer uniquement les bits transmis par la carte sans contact.

La figure V.13 illustre les différentes phases du lecteur bruité (de l'envoi de sa requête à la récupération de la trame envoyée par la carte).

Les avantages d'une telle solution par rapport à celles décrites dans la littérature ([CAS2006]) sont l'utilisation d'un bruit analogique, la non-modification des standards et du front-end RF de la carte.

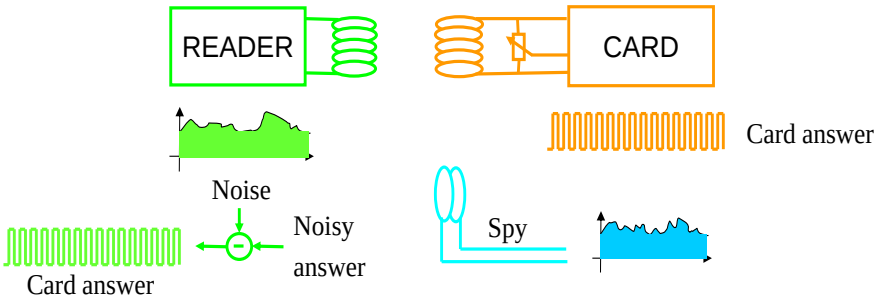


Figure V.13 – Le principe du lecteur bruité

Le lecteur bruité a été entièrement développé et implémenté sur une ancienne version du lecteur d'expérimentation Lrfv7 développé au CEA-Léti. Les figures V.14 et V.15 montrent le lecteur bruité, en particulier son générateur de bruit analogique et son antenne d'émission. Les modifications analogiques et numériques du lecteur Lrfv7 permettant l'ajout d'un bruit dans le canal sans contact vont être détaillées. Ce lecteur permet de bruiter le protocole ISO14443-B pour un débit de données de 106 kbits/s.

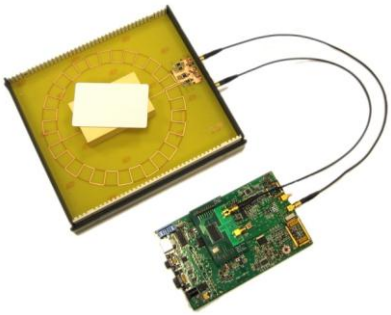


Figure V.14 – Le lecteur bruité et son antenne marguerite (sans amplificateur)

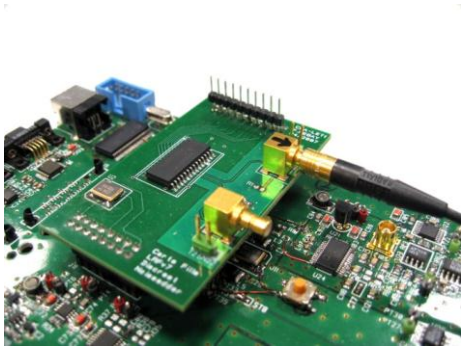


Figure V.15 – Le générateur de bruit

a. La partie numérique

La partie numérique du lecteur bruité génère un nombre aléatoire modulé à la fréquence porteuse du système sans contact (figure V.16). Cette partie est implémentée sur un composant programmable FPGA de type ALTERA Cyclone II intégré au lecteur Lrfv7.

La séquence pseudo-aléatoire est générée sur la base de trois cellules Tausworthe utilisant le principe du LFSR (Leap Forward Shift Register). La graine de démarrage de ces cellules est obtenue par une horloge externe décorélée de l'horloge de notre FPGA. Un nombre aléatoire est envoyé toutes les 9.44 µs, soit la durée d'un bit. Il permet de définir l'amplitude et la phase de la porteuse à 13.56 MHz de notre bruit (seule la modulation en amplitude est implémentée). La porteuse est modulée par une sous-porteuse à 847 kHz afin que le signal bruité coïncide avec le signal de la carte sans contact.

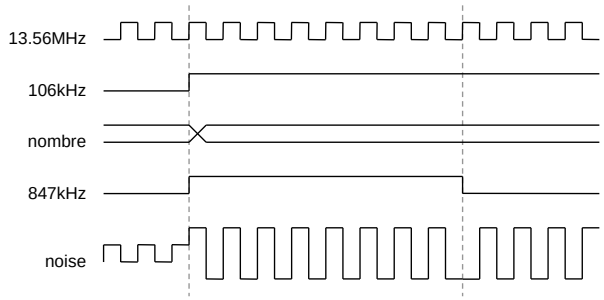


Figure V.16 – Génération du bruit modulé numérique

Pour récupérer un signal filtré à partir du signal bruité, il est nécessaire de numériser un signal bruité de référence pour connaitre le gain entre le bruit en émission et celui en réception. La soustraction du bruit au signal permet alors de retrouver un signal propre.

b. La partie analogique

La partie analogique convertit le signal bruité numérique modulé, l'amplifie et le transmet à l'antenne marguerite (figure V.17). Le signal bruité numérique sous porteuse sert d'entrée à un convertisseur 8 bits HI5690 (DAC) permettant d'obtenir un signal analogique. Ce signal est ensuite atténué pour servir d'entrée à un amplificateur RF mini-circuits ZHL-32A. La brique de base du lecteur bruité est son antenne appelée antenne marguerite. Ce design, étudié dans la section « Antenne marguerite », dispose de deux antennes en mutuelle nulle pour émettre le

champ et injecter le bruit séparément. Cette forte isolation entre les deux boucles inductives (40 dB) permet de réduire le bruit récupéré par la partie réception du lecteur lors de l'écoute de l'étiquette. Le traitement numérique du signal en réception est ainsi facilité.

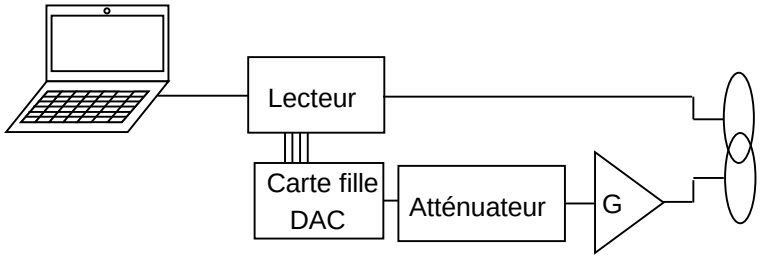


Figure V.17 – La partie analogique du lecteur bruité

c. Les améliorations possibles

Le lecteur actuel comporte plusieurs faiblesses que nous espérons corriger dans cette partie.

- Le lecteur bruité ne permet pas de bruiter n'importe quel protocole de communication sans contact
- L'antenne marguerite est très importante pour récupérer le signal, mais elle est difficilement industrialisable et implémentable sur tous les systèmes sans contact. Un énorme point fort du lecteur bruité serait l'utilisation d'une antenne standard (ISO10373-6) comportant une boucle inductive unique.
- L'atténuateur variable est actuellement manuel et l'amplitude du bruit ne s'adapte pas à la distance entre le lecteur et la carte sans contact.
- La synchronisation de la sous-porteuse de la carte avec celle du bruit n'est pas fiable

Toutes les solutions n'ont pas été implémentées, mais un grand nombre d'idées sont proposées dans cette partie.

3. L'émission de bruit

A. Choix des caractéristiques du bruit à générer

Le bruit généré par notre lecteur doit posséder des caractéristiques de tel sorte qu'un attaquant ne puisse pas retrouver les données émises par la carte à partir du champ magnétique récupéré par une antenne quelque soit sa position :

- A partir du signal bruité, l'attaquant ne peut pas retrouver le signal avant et après un passage par le canal sans contact.
- La bande spectrale du bruit doit entièrement recouvrir celle de notre signal. Quelle que soit la fréquence, la densité spectrale de puissance du bruit doit être supérieure à celle du signal. L'utilisation de filtres passe-bande ne doit pas permettre d'extraire le signal utile du bruit. Pour obtenir un tel bruit, il suffit de choisir un bruit dont la densité spectrale de bruit est la même que celle du signal utile. Un codage et une modulation similaires au signal utile permettent d'obtenir de telles caractéristiques. L'amplitude de ce bruit devra être suffisante pour brouiller le signal de la carte sans contact, mais limitée pour que le lecteur retrouve le signal dans ce bruit.
- Le bruit doit être généré de façon aléatoire de telle sorte qu'un attaquant ne puisse pas ni générer ce bruit, ni le prévoir. La connaissance du bruit à un temps T ne doit pas permettre d'identifier le bruit à un temps supérieur à T.

Le bruit généré par notre lecteur doit empêcher un attaquant de détecter les différents symboles envoyés par la carte. En étudiant les différentes normes sans contacts, il apparait

clairement que toutes ces cartes utilisent une fréquence sous porteuse. De plus, la modulation de charge de la carte sans contact introduit une modulation en amplitude du champ magnétique généré par le lecteur.

Les figures V.18 et V.19 représentent les FFT des différents signaux envoyés par les normes sans contact ISO14443 (type A et B) et ISO15693 en présence ou non de la modulation. On remarque nettement l'influence des fréquences sous porteuses à 424 kHz (ISO15693) et 847 kHz (ISO14443) sur la bande spectrale des signaux générés par la carte sans contact.

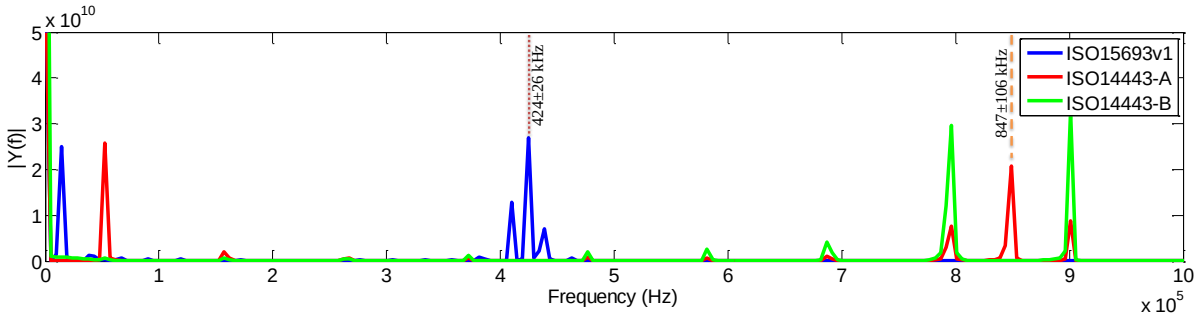


Figure V.18 – FFT des signaux codés des différentes normes

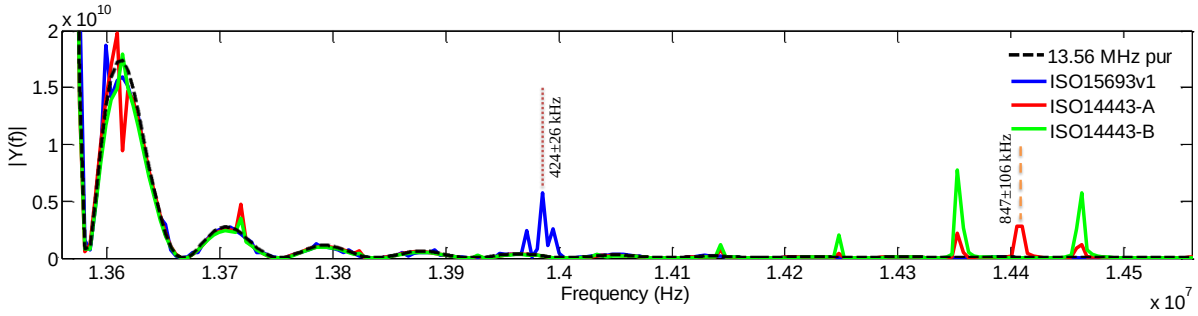


Figure V.19 – FFT des signaux codés et modulés des différentes normes

Pour générer un bruit susceptible de brouiller des signaux issus d'une de ces normes, le lecteur devra générer une porteuse modulée en amplitude par un signal possédant une fréquence sous porteuse. L'amplitude de cette modulation sous porteuse doit être aléatoire et modifiée à chaque symbole émis par la carte. Ainsi, en reproduisant la modulation et le codage de la carte au niveau du lecteur, le bruit recouvre entièrement la bande spectrale du signal. Nous avons implémenté un bruit basé sur le codage et la modulation du lecteur sous Matlab. Deux scénarios ont été étudiés :

- Le lecteur génère le bruit dans le canal sans contact. On mesure et on calcule la FFT du signal reçu sur une antenne de calibration.
- Le lecteur génère juste la porteuse du signal et une carte sans contact répond en modulation de charge (norme ISO15693). On mesure et on calcule la FFT du signal reçu sur une antenne de calibration.

On réalise cette expérience pour différents couplages pour être sûr d'obtenir le même résultat quel que soit la distance entre le système sans contact et la bobine de calibration.

Les courbes de la figure V.20 montrent que la densité spectrale de puissance du bruit est bien supérieure à celle du signal carte quelque soit le couplage entre les antennes.

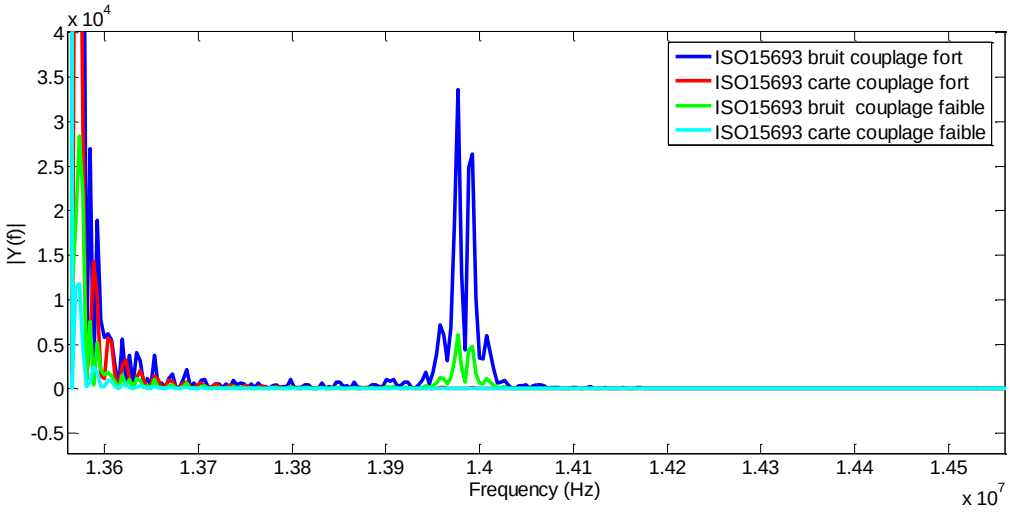


Figure V.20 – Comparaison entre FFT des signaux de la carte et celles du bruit

B. La synchronisation

Une première problématique non abordée dans la première version du lecteur bruité est la synchronisation du bruit avec le signal de la carte. Pour parvenir à récupérer la réponse de la carte, le lecteur bruité doit parfaitement synchroniser la sous-porteuse de la carte avec celle de son bruit. Nous proposons ici un protocole permettant de synchroniser notre signal.

Actuellement, aucune synchronisation automatique n'est réalisée par le lecteur bruité. Or, cette synchronisation est nécessaire car il existe des délais liés à l'émission du bruit et la réception du signal. L'envoi de la sous-porteuse du bruit lors de la détection de celle de la carte ne permet pas de faire concorder le bruit et le signal. Dans la version actuelle du lecteur, le bruit est généré un temps fixe après la réception de la sous-porteuse. Ce temps est mesuré de façon à obtenir la meilleure synchronisation entre les deux signaux à partir de la détection de la fréquence sous porteuse de la carte.

Nous avons imaginé et développé un nouveau protocole de synchronisation permettant de se synchroniser de façon bien plus précise avec la sous-porteuse de la carte. Le lecteur échantillonne le signal et détecte la sous-porteuse de la carte en mesurant des différences d'amplitude correspondant à la modulation de charge. Il génère alors une horloge synchronisée sur les fronts montants de cette réponse carte à la fréquence de la sous-porteuse. A partir de cette horloge, il crée une horloge désynchronisée permettant d'étudier les différentes positions et les différents déphasages entre cette horloge et la sous porteuse de la carte. Avec cette technique, il est possible d'obtenir un déphasage très faible entre les signaux lorsque la synchronisation a été effectuée. Ce déphasage minimal dépend du nombre de périodes de sous porteuse utilisables par notre lecteur avant que la carte émette une trame. La figure V.21 montre un exemple de synchronisation lorsque 4 périodes de sous-porteuses sont utilisables par notre phase de synchronisation. Pendant chacune de ces périodes de sous porteuses, l'horloge générant la sous-porteuse de notre bruit est décalée d'un quart de la période de sous-porteuse. Ainsi, on échantillonne le champ magnétique résultant pour quatre positions différentes de la sous-porteuse du bruit. On mesure la valeur de corrélation pour ces quatre positions de façon à identifier le déphasage présentant la forme la plus propre de modulation d'amplitude. En bas de la figure V.21, on peut observer la frise identifiant le nombre d'échantillons semblables pour chacune de ces périodes. Dans ce cas, c'est la position 1 qui semble la plus intéressante. Cependant, le nombre de périodes de sous-porteuse disponibles est trop faible pour obtenir un taux d'échantillons valides permettant un déphasage très faible.

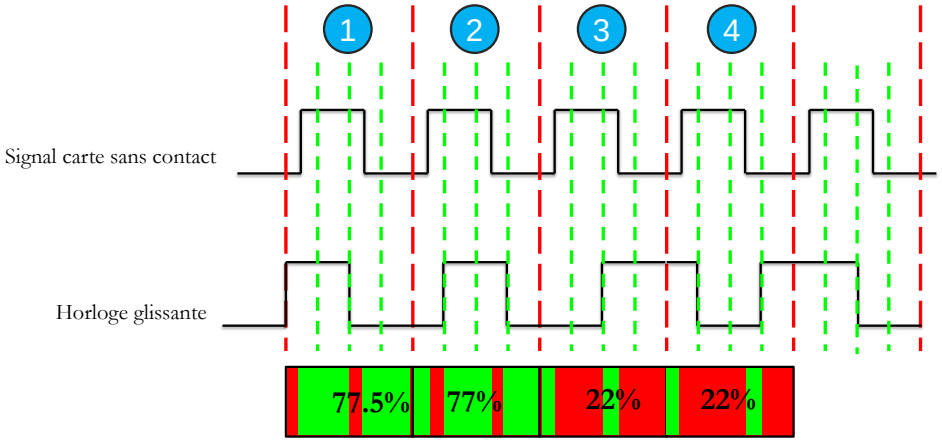


Figure V.21 – Phase de synchronisation sur 4 périodes

La figure V.22 montre la même solution avec un nombre de 16 périodes de sous-porteuse disponibles. Ainsi, la précision de notre protocole est bien plus grande : un seizième de la période de la porteuse. On peut atteindre des taux de réponses valides proche des 100%. En numérique, le déphasage théorique limite est la fréquence d'échantillonnage. En pratique, le signal modulé n'est pas carré car le canal sans contact est lent donc on n'obtiendra jamais ou rarement un taux d'échantillons valides aussi important.

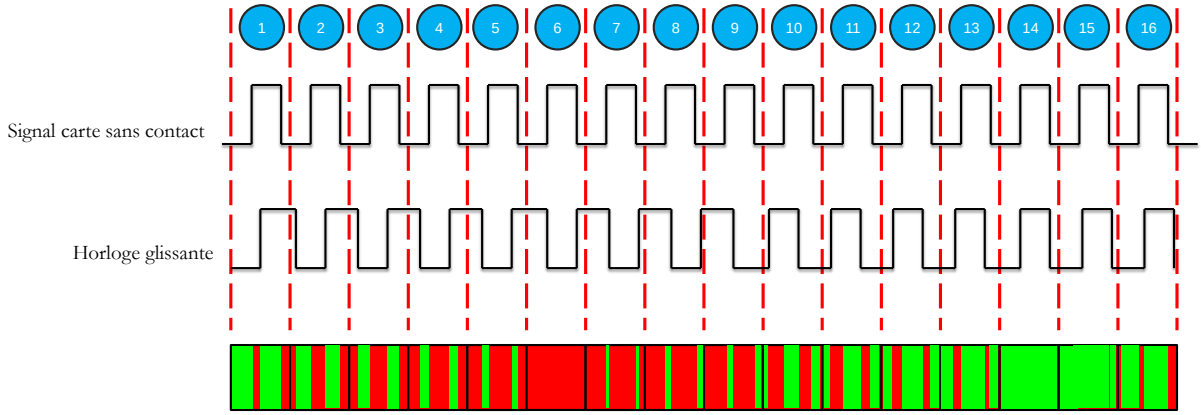


Figure V.22 – Phase de synchronisation sur 16 périodes

La synchronisation doit être réalisée le plus tôt possible de façon à obtenir un bruit en concordance avec la réponse de la carte. Cependant, cette synchronisation ne peut pas commencer avant que la carte n'émette sa sous-porteuse. Le début de la réponse carte correspond au début de la trame (SOF) ; cette période va permettre de réaliser la phase de synchronisation. Les figures V.23 et V.24 montrent respectivement cette phase pour les normes ISO15693 et ISO14443-B. On observe durant cette période les différents déphasages entre le signal de la carte et le bruit qui crée des variations au niveau de l'amplitude de la sous-porteuse. A la fin de cette phase, le lecteur calcule la position la plus en phase et l'utilise pour synchroniser.

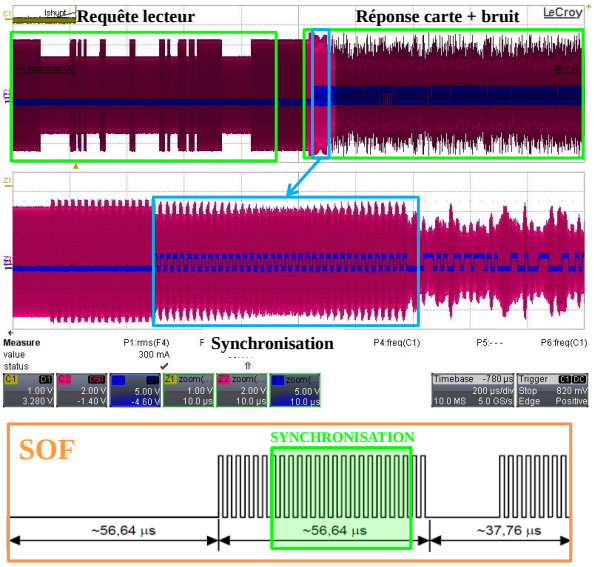


Figure V.23 – Phase de synchronisation en ISO14443-B

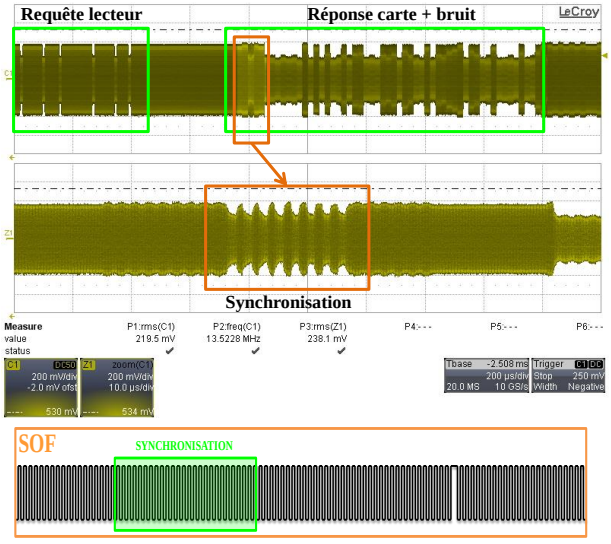


Figure V.24 – Phase de synchronisation en ISO15693

Nous n'avons pas identifié de solution pour la norme ISO14443-A car cette norme ne présente pas suffisamment de période de sous porteuse pour se synchroniser avant la trame du message.

C. Synchronisation de phase entre le signal bruité et le signal du lecteur

La solution utilisant les antennes marguerites consiste à générer la porteuse du signal permettant d'alimenter la carte sans contact sur une antenne inductive et le bruit sur l'autre boucle inductive. Pendant nos différents tests, nous avons pu observer que le taux de réponse de la carte était assez faible lorsque le bruit était actif. Le champ magnétique généré par les deux boucles inductives est cependant propre donc on peut penser qu'il n'y a pas de déphasage entre les signaux des deux boucles inductives. Pourtant, les deux signaux sont générés par la même horloge du FPGA mais leur circuit d'émission est très différent. L'analyse des signaux en entrée des antennes marguerite a permis de montrer un important déphasage lorsque la carte ne répond pas (comme en témoigne les figures V.25 et V.26)

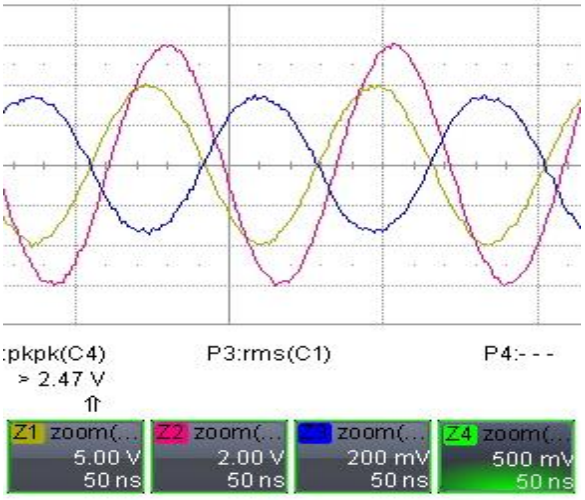


Figure V.25 – Déphasage lorsque la carte répond (Bleu : champ RF ; jaune : signal porteuse et en rouge : bruit généré)

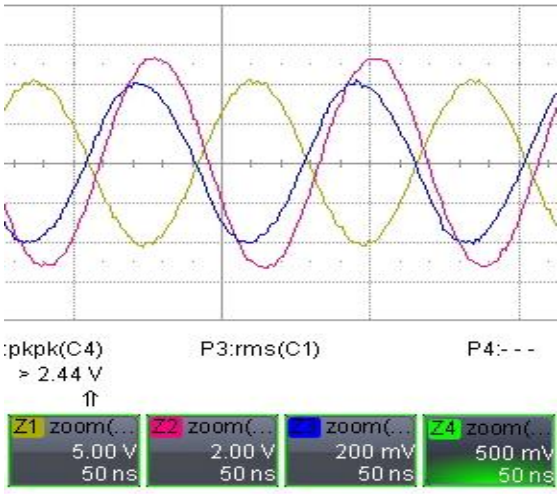


Figure V.26 – Déphasage lorsque la carte ne répond pas (Bleu : champ RF ; jaune : signal porteuse et en rouge : bruit généré)

Ce déphasage entre les deux signaux émis est un réel problème puisque la carte ne répond pas lorsque ces signaux sont déphasés et qu'il n'est pas possible de prévoir la valeur de ce déphasage. Une solution consiste alors à mesurer la différence de phase entre les deux signaux. Ainsi il est possible de diminuer le déphasage et augmenter le taux de réponse de la carte. Nous avons identifié le circuit AD8302 qui permet de mesurer la différence de phase entre deux signaux de fréquence inférieure à 2,7 GHz (figures V.27 et V.28). La fréquence de la porteuse des deux signaux analysés est de 13,56 MHz ; ce circuit est suffisant pour détecter la différence de phase entre nos signaux. Ce circuit a une précision dans la mesure de phase de 10 mV/°. Pour notre système, un tel niveau de précision n'est pas nécessaire et il sera possible de remplacer ce circuit à solution plus simple.

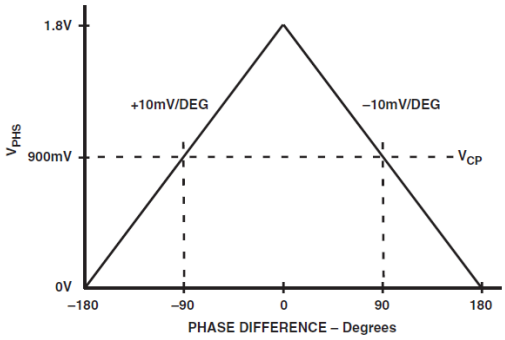


Figure V.27 – Résultats de la mesure de phase sur la sortie du circuit

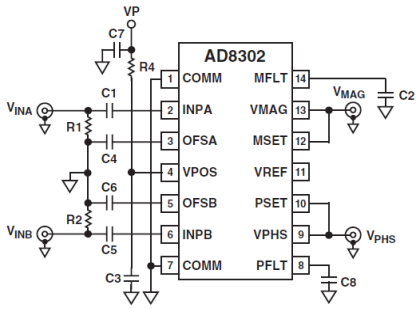


Figure V.28 – Composant de mesure de phase

Le circuit mesurant la différence entre les deux signaux donne une tension analogique comprise entre 0 et 1.8V. Cette tension doit être convertie au format numérique car cette donnée va permettre de resynchroniser les deux signaux à 13.56MHz. On utilise donc un convertisseur analogique numérique (CAN). Toute la partie traitement, analyse et réaction est réalisée en VHDL. En fonction de la valeur du décalage de phase, notre système peut en déduire le décalage à ajouter pour que les deux signaux soient synchronisés. Cette étape doit bien sûr être réalisée dès que l'on active le bruit modulé, c'est-à-dire après la fin de la trame de la requête du lecteur. La figure V.29 présente le système de mesures complet.

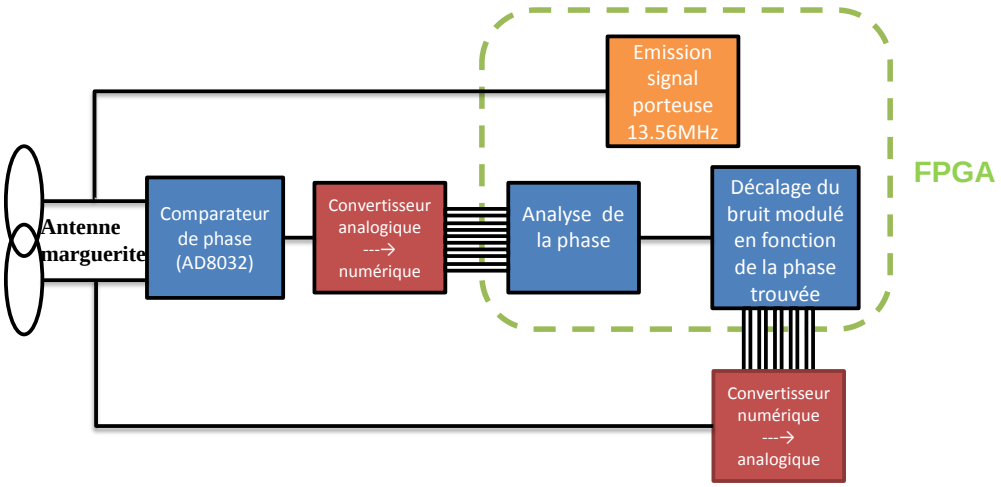


Figure V.29 – Synoptique du système de mesure et d'analyse

Le système peut être vu comme un système d'asservissement (figure V.30). Le comparateur permet de mesurer l'erreur de phase entre les deux signaux et le FPGA permet de corriger cette erreur pour qu'elle tende vers zéro. Cependant, l'horloge maximale de traitement de notre FPGA

étant de 216 MHz, la précision de cette erreur sera de 5 ns. Cette valeur est négligeable devant la période la porteuse qui est de 73.74 ns.

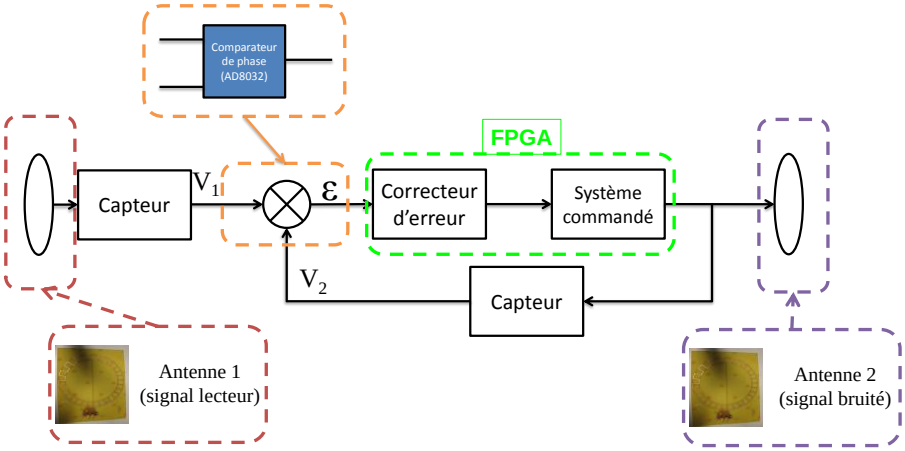


Figure V.30 – Asservissement du système en phase

Il existe plusieurs possibilités permettant de simplifier le système :

- Remplacer le convertisseur par un simple comparateur. On modifie la phase des signaux tant que la valeur de l'erreur est plus grande qu'une certaine référence paramétrée.
- Remplacer le circuit mesurant la différence de phase par de simples comparateurs permettant d'analyser les positions des zéros des deux signaux sinusoïdaux.

D. Optimalisation de l'amplitude de bruit

La valeur de l'amplitude du bruit est très importante puisqu'elle doit être suffisante pour brouiller le signal de la carte, mais assez faible pour que le lecteur parvienne à détecter la réponse de la carte dans le bruit. Selon la distance entre le lecteur et la carte, il peut aussi être nécessaire d'augmenter ou de diminuer la valeur de l'amplitude du bruit. En effet, plus la carte est loin et plus le lecteur doit émettre un bruit de forte amplitude pour brouiller le champ magnétique à proximité de la carte.

Dans la version du lecteur bruité actuel, cette optimisation de l'amplitude du bruit est réalisée à l'aide d'un atténuateur variable manuel placé avant l'amplificateur RF.

Nous proposons une solution automatique basée sur l'analyse du couplage entre le lecteur et la carte et sur une amplification automatique de la chaine d'émission du bruit.

Le coupleur directionnel positionné entre l'antenne et les modules d'émission et de réception permet de mesurer l'influence de la carte sur le lecteur. La modulation de charge de cette carte et sa position dans le champ magnétique du lecteur modifient la charge équivalente de l'antenne. La modification de cette charge est vue en sortie du coupleur sur la chaine de réception. Plus le signal en sortie du coupleur est faible et plus la carte est en couplage faible avec le lecteur. La chaine de réception du lecteur a été développée de façon à obtenir un signal de même amplitude en entrée du convertisseur analogique numérique quelque soit l'amplitude du signal en sortie du coupleur. Pour asservir la valeur de cette amplitude, un amplificateur de gain variable commandé par le FPGA permet d'amplifier ou d'atténuer la tension en entrée du convertisseur (figures V.31 et V.32). La valeur de ce gain permet donc d'obtenir une indication sur la valeur du couplage entre l'antenne lecteur et l'antenne carte. A partir de la valeur numérique de ce gain, le lecteur en déduit la valeur de l'amplitude du bruit nécessaire pour bruiter le signal. Une calibration sera préalablement nécessaire de façon à savoir quel gain en réception équivaut à quel couplage entre le lecteur et la carte. L'atténuateur manuel est remplacé par un amplificateur à gain variable

commandé par le FPGA via un bus SPI. La valeur d'amplification de ce préamplificateur variable dépend donc directement du couplage entre les antennes du lecteur et de la carte.

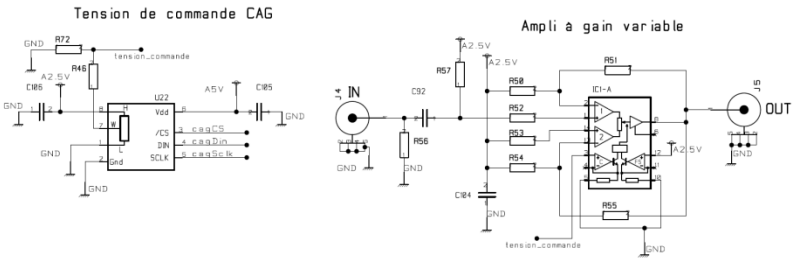


Figure V.31 – Electronique du circuit d'optimisation du gain

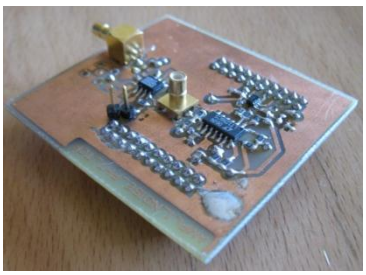


Figure V.32 – PCB du circuit de contrôle de gain

E. Suppression de l'antenne marguerite

La problématique la plus importante du lecteur bruité est l'utilisation d'antennes marguerites. Ces antennes sont assez complexes à réaliser et ne sont pas industrialisables pour le moment. Notre objectif est donc de remplacer ces antennes par une simple antenne à boucles inductives conforme avec la norme ISO 10373-6. Pour générer le bruit, l'idée la plus simple est de moduler le champ magnétique émis par le lecteur de manière aléatoire lorsque la carte répond. Cette modulation d'amplitude peut être réalisée par la commutation des transistors utilisées lors de la phase d'émission du lecteur (voir « Carte fille lecteur bruité : modulation d'amplitude »). Ainsi, aucune modification du front-end RF du lecteur n'est nécessaire pour réaliser le bruit. La figure V.33 est une représentation simplifiée du lecteur obtenu.

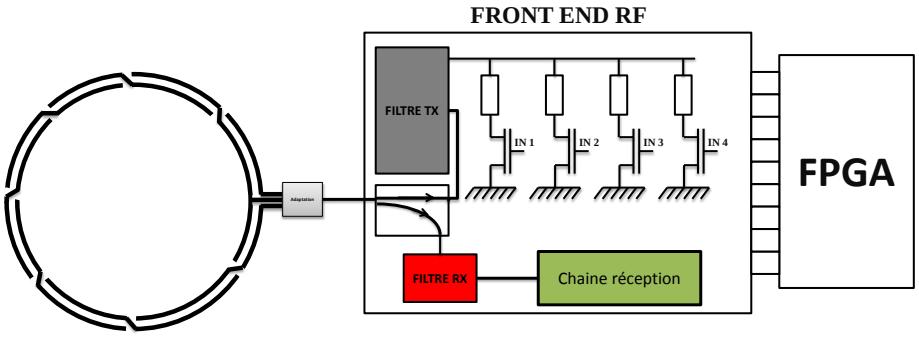


Figure V.33 – Lecteur bruité sans antenne marguerite

Les figures V.34 et V.35 montrent les résultats obtenus pour un tel système. Comme on peut l'observer sur la figure V.34, l'émission du bruit ne pose aucun problème. Pendant la phase de synchronisation, l'amplitude du bruit est constante. Ensuite, l'amplitude du bruit est aléatoire ; un attaquant ne peut pas discerner les différents bits émis par la carte sans contact dans ce champ magnétique. Il a été observé que les échantillons récupérés à la sortie du convertisseur analogique numérique de la chaine de réception ne permettaient pas de retrouver le signal de la carte sans contact dans le bruit. La figure V.35 montre le signal au niveau d'une bobine de calibration (en bleu) et les signaux obtenus au niveau de la chaine de réception, juste avant le convertisseur de données. On peut remarquer d'importants phénomènes transitoires pour chaque modification de la consigne du bruit. Ces perturbations sont obligatoirement introduites par notre chaine de réception puisque le champ magnétique au niveau de la bobine de calibration est propre. Il est donc nécessaire d'analyser les différents modules de la chaine de réception pour comprendre ces phénomènes.

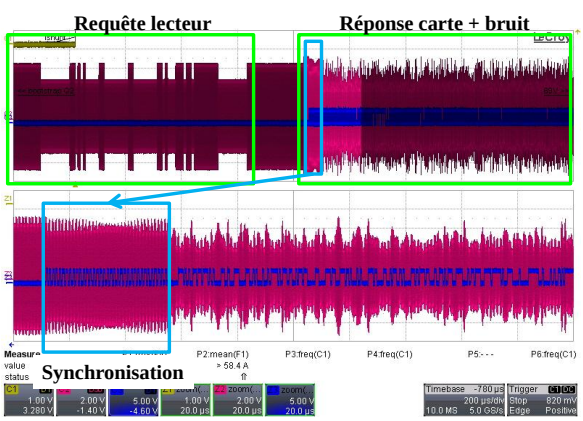


Figure V.34 – Effet du bruit sur le champ magnétique

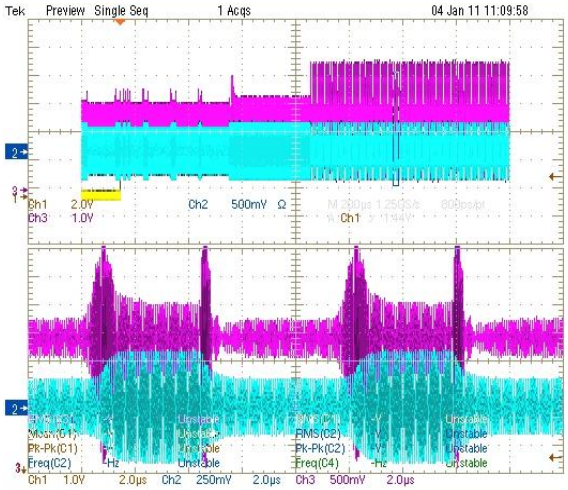


Figure V.35 – Phénomènes transitoires sur la chaine de réception du signal

Le coupleur directionnel de notre lecteur est le composant qui génère ces phénomènes transitoires. Théoriquement, un coupleur directionnel permet de mesurer le courant dans une ligne de transmission sans la perturber. Une partie du signal traversant le coupleur est prélevée et mise en sortie du coupleur directionnel. Dans notre cas, le signal est injecté par l'entrée standard, mais aussi par la sortie. Deux tests ont été réalisés (figures V.36 et V.37); ils permettent de montrer l'influence d'un signal en sortie du coupleur sur le signal récupéré sur la sortie BACK du composant. Le signal rose représente le signal enregistré avec l'oscilloscope sur le BACK du coupleur. Comme on peut le constater, l'injection d'un signal en sortie du coupleur introduit de grosses perturbations lors des transitions du signal.

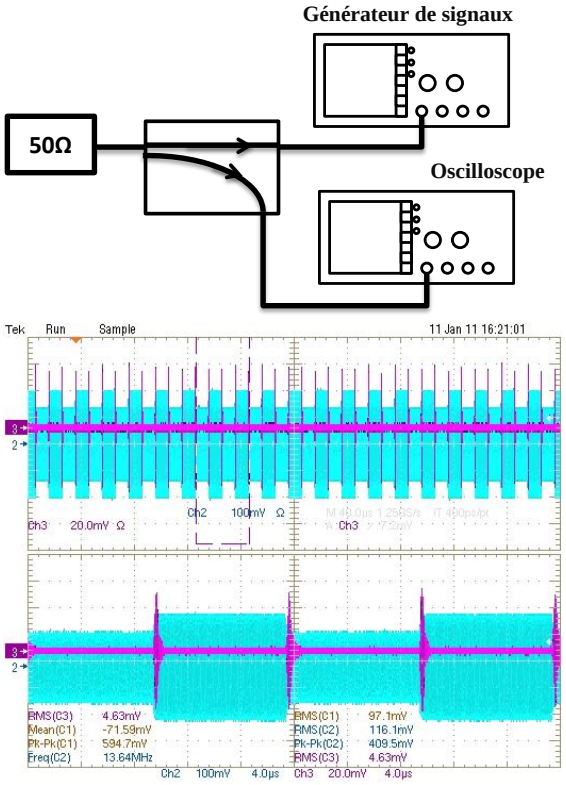


Figure V.36 – Test 1 et résultats du test 1 (bleu : champ RF ; rose : sortie BACK coupleur)

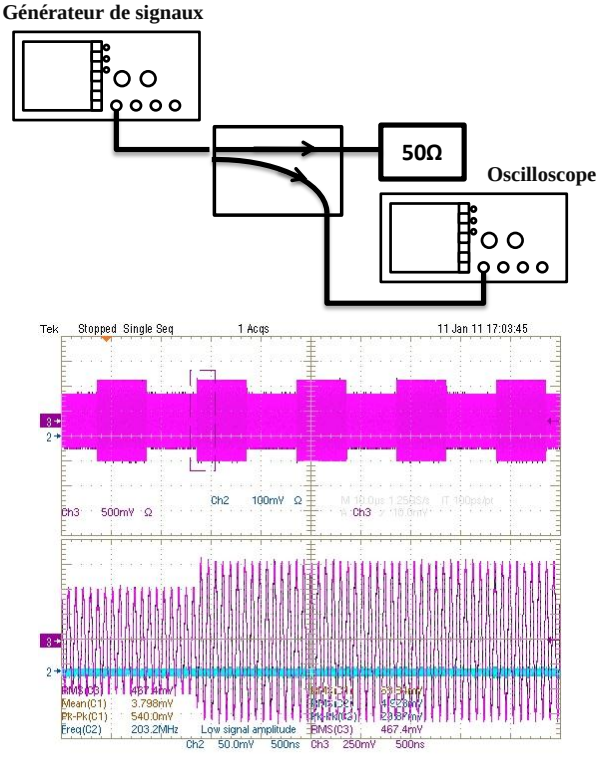


Figure V.37 – Test 2 et résultats du test 2 (rose : sortie BACK coupleur)

A partir des tests réalisés, on peut conclure que le bruit ne doit pas être généré par le lecteur existant, mais par un autre module. Ainsi, on écarte le coupleur de notre chaine d'émission de bruit. A partir de ces résultats, nous avons identifié deux nouvelles solutions permettant d'émettre un signal bruité. Ces deux solutions sont articulées autour d'un transformateur à trois enroulements :

- Le premier enroulement est connecté à l'antenne ISO103873-6.
- Le deuxième enroulement est connecté à la sortie RF du lecteur.
- Le troisième enroulement est connecté à la sortie de la carte fille.

La première solution consiste à moduler le champ magnétique émis par le lecteur à l'aide de transistors Mosfets (figure V.38). Ces transistors sont routés sur une carte fille et permettent de faire commuter des charges de différentes valeurs. Cette solution est très proche de la première solution développée qui ne fonctionnait pas. L'avantage de cette solution est qu'on limite les phénomènes transitoires liés au coupleur directionnel. La modulation de champ est donc effectuée derrière l'entrée du coupleur.

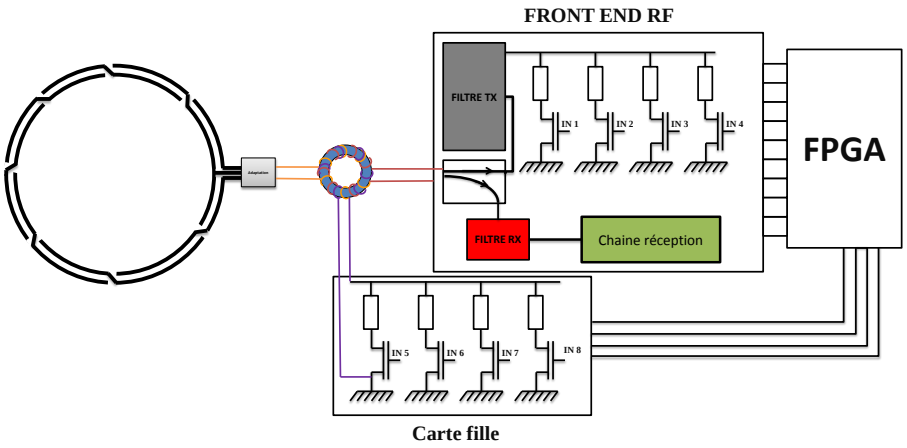


Figure V.38 – Lecteur bruité avec carte de modulation d'amplitude par Mosfets

Dans ces deux solutions, le transformateur à 3 enroulements permet de connecter deux signaux d'entrée comme il était possible de le faire avec l'antenne marguerite. La deuxième solution consiste donc à utiliser la partie analogique développée par l'équipe du CEA (convertisseur de données + amplificateur HF) (figure V.39). La sortie de cette carte analogique est connectée à un des enroulements du transformateur. Il est possible d'utiliser cette carte pour générer le champ radiofréquence, l'émission des requêtes lecteur et du bruit. Il est donc possible de supprimer toute la chaine d'émission de données du lecteur actuel.

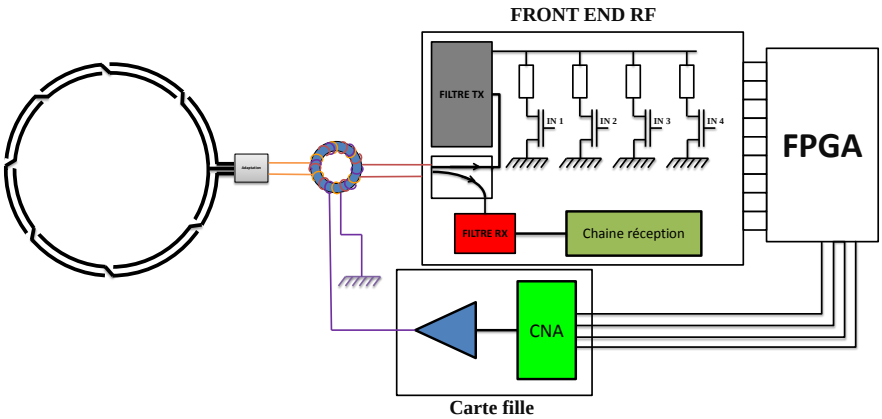


Figure V.39 – Lecteur bruité avec carte de modulation d'amplitude par CNA

Ces deux solutions n'ont pas donné les résultats espérés. En effet, le signal en entrée du convertisseur analogique-numérique de la chaine de réception est légèrement perturbé. Le plus gros problème reste la difficulté à retrouver le signal de la carte dans le bruit. En effet, une telle méthode introduit un couplage fort entre la chaine de réception et d'émission du bruit. Alors que l'antenne marguerite de réception atténuait fortement le bruit émis, l'enroulement de réception du transformateur est directement couplé à l'enroulement d'émission du bruit. Il n'est donc pas possible de récupérer le signal faible provenant de la carte dans une modulation d'amplitude dont l'index de modulation est important. Les essais utilisant une unique antenne inductive ont donc été arrêtés à la suite de ces résultats.

F. Emission du bruit avec antenne marguerite

a. Première solution

Cette solution consiste à remettre à jour la version actuelle du lecteur bruité. La partie analogique reste la même (CNA + amplificateur); on modifie la partie numérique (figure V.40). Le bruit généré est différent et on a modifié la méthode de synchronisation.

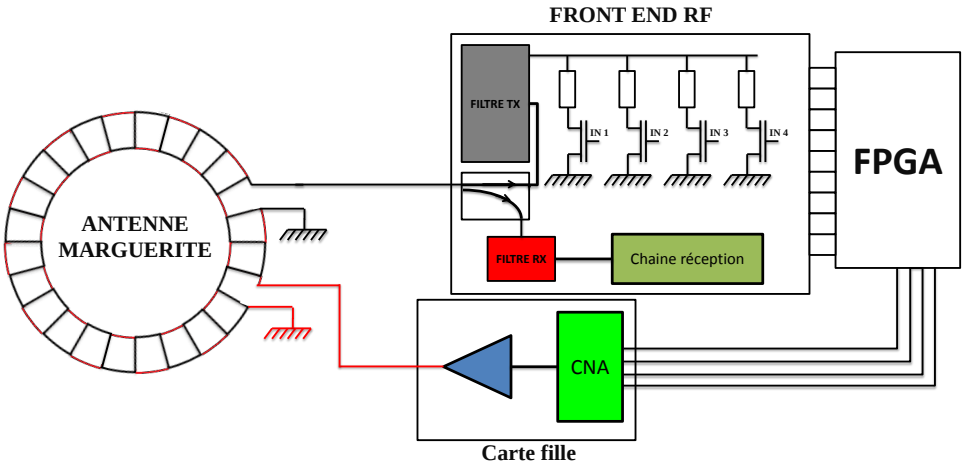


Figure V.40 – Lecteur bruité avec antenne marguerite et modulation par CNA

La figure V.41 présente les résultats obtenus ; les échantillons en sortie du convertisseur, la moyenne de ces échantillons sur une période de sous-porteuse et la consigne de bruit ont été enregistrés à l'aide d'un analyseur logique. Comme on peut le remarquer, la moyenne des échantillons semble suffire pour décoder le signal de la carte. Le bruit émis par le lecteur est assez atténué par l'antenne marguerite et il n'est pas nécessaire de soustraire la consigne de bruit au signal récupéré. La comparaison de cette moyenne avec un seuil fixe ou variable permet d'obtenir le signal démodulé en rouge correspondant parfaitement au signal non décodé de la carte.

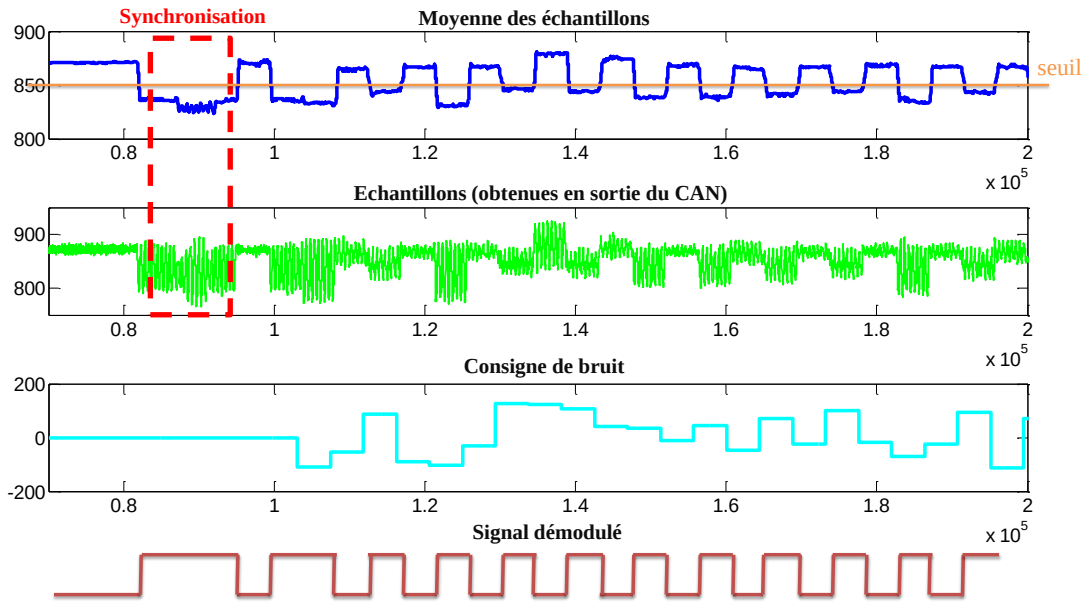


Figure V.41 – Résultats obtenus : à partir de la moyenne des échantillons, on récupère facilement le signal démodulé

Cette solution est très intéressante puisqu'aucune démodulation complexe du signal n'est requise ; le signal est directement récupéré malgré le bruit. L'antenne marguerite atténue suffisamment le bruit. Actuellement, la solution implémentée permet uniquement de décoder la réponse ; le signal n'est pas envoyé jusqu'au microcontrôleur chargé d'analyser les réponses de la carte. Pour cette solution, il est nécessaire d'implémenter le système avec asservissement de la phase car deux signaux déphasés sont injectés dans les antennes marguerites et la carte ne répond pas tout le temps.

b. Deuxième solution

La deuxième solution développée consiste à modifier l'utilisation de l'antenne marguerite. Dans le lecteur actuel, l'une des entrées de l'antenne est utilisée pour la porteuse et la réception du signal de la carte tandis que l'autre entrée est utilisée pour émettre le bruit. L'implémentation suivante propose d'utiliser la première antenne pour l'émission du bruit et de la porteuse et utiliser la seconde entrée uniquement pour la réception. Nous avons décidé de reprendre l'idée d'utiliser les transistors Mosfets du lecteur pour générer le bruit (figure V.42).

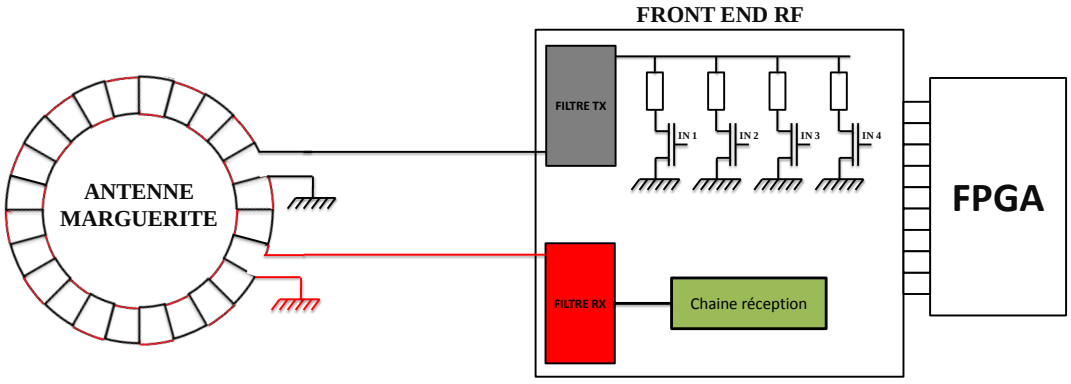


Figure V.42 – Lecteur bruité avec antenne marguerite et modulation par transistors Mosfets

Cependant, il est aussi possible d'utiliser un CNA pour générer à la fois le bruit et la porteuse. L'analyse du champ magnétique à l'aide d'une bobine de calibration permet de constater que la

génération de bruit ne pose aucun problème et que la synchronisation se fait correctement (figure V.43). Le bruit est aléatoire et aucune sonde de champ ne peut détecter le signal de la carte en analysant le signal enregistré.

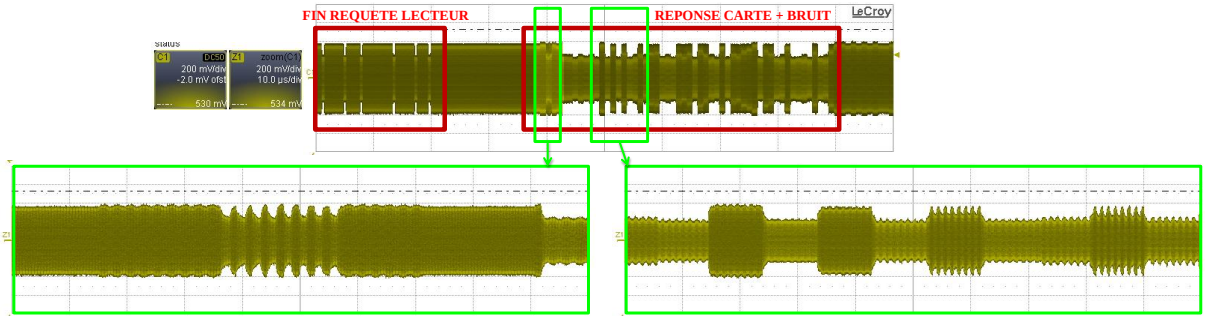


Figure V.43 – Champ magnétique lors de l'émission du bruit à l'aide de transistors Mosfets

Le Proxispy est un analyseur de trames émises par des systèmes sans contact conformes aux normes ISO14443-A, ISO14443-B et ISO15693. Cet outil permet d'extraire le signal dans le bruit grâce à un design d'antenne spécifique. Chacun des systèmes réalisés a été testé avec cet outil de façon à vérifier qu'un attaquant proche de la carte utilisant un design d'antenne spécifique n'est pas capable de retrouver le signal. Chacun de nos systèmes a permis d'obtenir le même résultat (figure V.44). On observe que la requête lecteur est bien comprise par le Proxispy (la commande 'inventory') ; la trame émise par la carte sans contact n'est pas décodée.

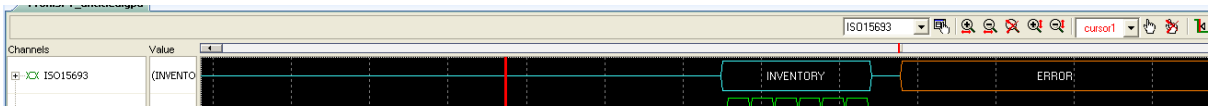


Figure V.44 – Résultats du Proxispy

La figure V.45 montre les résultats obtenus au niveau de la chaine de réception. Les signaux ont été enregistrés à partir d'un analyseur logique. Les courbes montrent les échantillons enregistrés pendant le début de la réponse carte et la consigne de bruit (signaux envoyés aux différents transistors).

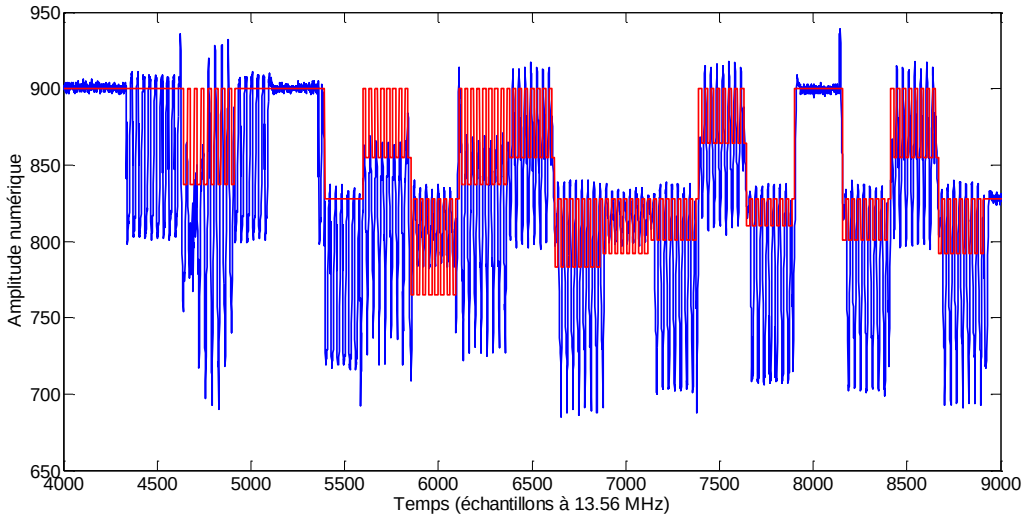


Figure V.45 – Résultats obtenus (bleu : échantillons en sortie du CAN ; rouge : consigne de bruit)

On reconnait la phase de synchronisation au début de cette trame avec un signal perturbé. Le signal est ensuite relativement propre. L'observation intéressante est la forte corrélation entre la

consigne de bruit envoyée aux transistors et les échantillons récupérés en sortie du convertisseur analogique numérique. Malgré la non-linéarité du bruit généré par les différentes charges modulées des transistors, cette utilisation de l'antenne marguerite semble être prometteuse. Il s'agit maintenant de remplacer la modulation par transistors et l'émission du champ RF par une carte avec un convertisseur numérique analogique et un amplificateur.

Au niveau de la chaine de réception, le lecteur doit séparer le bruit de la réponse de la carte. La solution consiste à estimer les convolutions subies par le bruit entre son émission et sa réception par le lecteur (figure V.46). Sur cette figure, H1 est le canal de communication sans contact.

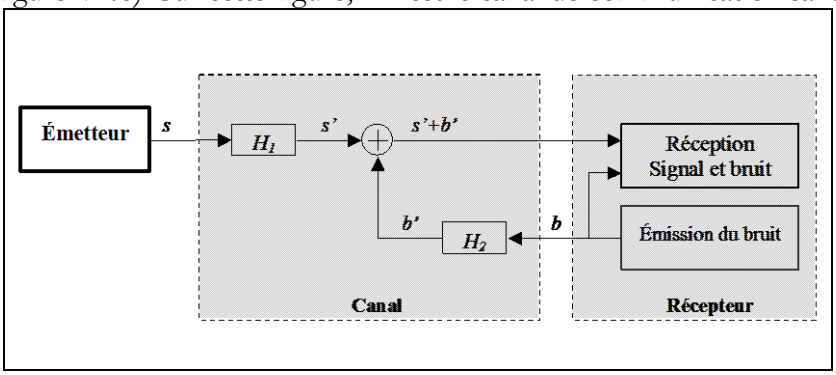


Figure V.46 – Convolutions subies par le signal et le bruit

Pour que le lecteur puisse éliminer le bruit b' à partir de la connaissance de la consigne de bruit b, il doit estimer la fonction de transfert H_2. Pendant le temps de retournement de la carte, le lecteur peut activer le bruit pendant une durée symbole de façon à identifier un bruit de référence et s'en servir pour évaluer le gain entre l'émission du bruit et sa réception.

En connaissant la valeur de ce gain, la soustraction du bruit devient simplifiée si la valeur de ce gain est linéaire en fonction de l'amplitude des sous-porteuses du bruit. Il suffit de soustraire la consigne de bruit modifiée par le gain calculé au signal en réception du lecteur.

Cette chaine de démodulation reste donc la même que dans la version actuelle.

Même si le démonstrateur n'est pas terminé, la plupart des développements existent à présent et il suffit de regrouper les différents modules existants.

4. Conclusion du chapitre

Le lecteur bruité est un dispositif brouillant la communication entre une carte et un lecteur. Cette solution supprime tous les risques d'espionnage de la communication par un attaquant. Le bruit s'ajoute à la porteuse émise par le lecteur ; le champ magnétique est donc perturbé. Le lecteur peut retrouver la réponse de la carte sans contact par la connaissance de la consigne de bruit. Aucun autre dispositif de réception ne peut retrouver cette réponse. Dans ce chapitre, nous avons étudié plusieurs dispositifs permettant d'améliorer la puissance et la fiabilité de ce système. Nous avons ainsi montré qu'il n'était pas possible de remplacer les antennes marguerites par une simple boucle inductive car le rapport signal sur bruit devient alors trop faible. Cependant, nous avons pu proposer d'autres solutions d'émission de bruit permettant de simplifier le système actuel. Nous avons aussi résolu plusieurs problématiques comme le déphasage entre les porteuses des signaux ou l'optimisation du gain du bruit. Le lecteur bruité reste un dispositif complexe et nous n'avons pas réussi à développer un prototype complet pendant les derniers mois de la thèse. Les deux solutions développées sont envisageables. Cependant, nous pensons qu'il est préférable de privilégier la deuxième solution de façon à injecter un signal unique dans l'antenne marguerite. Pour cette solution, il est encore nécessaire de développer l'émission du signal et du bruit à l'aide d'un convertisseur numérique-analogique et de travailler sur le traitement de la réception afin d'extraire le bruit.

CONCLUSION GENERALE

1. Bilan Technique

Ce travail de thèse avait pour objectif la sécurisation de la couche physique des communications sans contact. Nous avons travaillé sur différents points de cette problématique de façon à proposer un panel de contre-mesures adaptées à ces systèmes.

Plusieurs attaques spécifiques au lien sans contact ont été implémentées de façon à identifier le matériel nécessaire par un attaquant et les limites liées à ces attaques. Plusieurs mesures d'eavesdropping ont été effectuées dans differents environnements (extérieur et intérieur) pour les différentes normes ISO (14443-A et B et 15693). Ces mesures ont permis de montrer qu'un attaquant était capable d'écouter les transactions envoyées par le lecteur à la carte à 200 fois la distance de fonctionnement du système. Trois types d'attaques relais ont été mises en place de façon à obtenir les délais les plus faibles de la littérature (jusqu'à quelques centaines de nanosecondes). Un relais plus perfectionné de type G. Hancke a aussi été réalisé permettant une démodulation complète du signal.

Nous avons étudié et développé trois contre-mesures permettant de détecter la présence d'un relais introduit dans un système sans contact.

La première de ces solutions est basée sur la mesure de temps par le calcul de la corrélation entre deux séquences. Cette technique mathématique est intégrée dans un protocole d'authentification permettant d'identifier la présence d'une carte valide en face du lecteur sans contact. Cet algorithme de détection de relais a été implémenté sur un système sans contact et a permis d'obtenir une résolution proche de 300 ns, nous permettant de détecter la plupart des attaques relais

La seconde solution utilise les caractéristiques de la couche physique pour détecter la présence de relais. Une étude théorique basée sur les équations du canal de communication d'un système sans fil a montré qu'il existe une différence entre les quantités de bruit avec et sans relais. Diverses études basées sur des signaux de bruits enregistrés sur oscilloscope et analysés sous Matlab ont été réalisées donnant lieu à des résultats difficiles à analyser. L'implémentation de l'algorithme sur un système sans contact d'expérimentation a permis de montrer que cette solution n'était pas adéquate pour les systèmes sans contact en raison de la non-linéarité du canal.

Cette troisième contre-mesure permet aussi bien l'authentification d'une carte que la détection d'un relais de type « amplify and forward ». Cette solution consiste à envoyer un échelon de forte amplitude dans l'antenne du lecteur de façon à obtenir une réponse de type oscillations amorties (les antennes lecteur et carte sont des circuits RLC). L'analyse de l'amortissement de ces oscillations peut permettre au lecteur de connaitre beaucoup d'informations sur les circuits oscillants en couplage fort avec lui. Des tests de simulations et des mesures expérimentales ont été réalisés de façon à valider cette première approche. Les résultats obtenus sont particulièrement intéressants mais cette solution nécessite encore beaucoup de travail.

Une partie de la thèse a permis de travailler sur l'amélioration d'un dispositif existant permettant de lutter contre l'attaque eavesdropping. Dans cette contremesure, un lecteur sans contact génère un bruit important lorsque la carte lui répond de façon à éviter toute écoute illicite de la part d'un espion. Cette solution a été précédemment réalisée par une équipe du CEA Léti ; elle est fonctionnelle, mais nécessite quelques améliorations. Par exemple, le lecteur doit générer à l'heure actuelle un champ RF permettant d'alimenter la carte mais aussi un champ RF bruité. Ces deux champs sont envoyés sur une antenne à deux boucles en mutuelle nulle de façon à éviter toutes perturbations entre les deux signaux. Des études par simulation ont été réalisées et de nouvelles architectures électroniques ont été développées. Les améliorations apportées ne sont pas encore fonctionnelles car il reste encore à développer certaines parties électroniques.

2. Avancées par rapport à l'état de l'art

Ce travail de thèse a permis de faire progresser la recherche dans le domaine de la sécurité des communications sans contact. Cette étude se démarque de l'état de l'art par ces différents résultats :

- Modélisation et réalisation de nouvelles attaques relais introduisant des délais inférieurs à la µs dans les systèmes sans contact.
- Développement et implémentation d'un démonstrateur permettant de détecter toutes les attaques relais existantes en mesurant les délais introduits.
- Analyse et étude d'un système basé sur la réponse indicielle et permettant la détection, l'authentification de cartes et la détection d'attaques relais de type 'amplify and forward'.
- Amélioration du système lecteur bruité permettant de brouiller la communication entre un lecteur et une carte sans contact.

3. Perspectives

Il reste encore du travail pour valider l'ensemble des contre-mesures que nous avons développées. Toutes les solutions n'ont pas été entièrement développées et de nombreuses voies d'améliorations sont possibles.

Pour la solution utilisant la corrélation, il est nécessaire d'implémenter le protocole d'authentification, mais il serait aussi intéressant de travailler sur un circuit de démodulation plus simple au niveau du récepteur.

Les résultats sur la réponse indicielle sont très bons et cette solution devra être intégrée dans le système sans contact d'expérimentations du CEA.

Les développements identifiés pour améliorer le lecteur bruité doivent être implémentés de façon à juger de leur efficacité

RÉFÉRENCES

[BIE2007] M. Bielmann, J.-P. Curty, *Contactless Card with membrane switch made of elasto-resistive material*, brevet US0290051, ASSA ABLOY Identification technology group, 2007.

[BRA1993] Stefan Brands, David Chaum: Distance-bounding protocols (extended abstract). Proceedings Eurocrypt '93, 1993.

[CAP2003] S. Capkun, L. Buttyan, J.-P. Hubaux, *SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks*, Processings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[CAR2005] D. Carluccio, K. Lemke, and C. Paar, *Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results*, Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, 2005.

[CAR2006] D. Carluccio, T. Kasper, and C. Paar, *Implementation Details of a Multi Purpose ISO 14443 RFID-Tool*, Workshop on RFID Security – RFIDSec'06, Austria, 2006.

[CAS2006] C. Castelluccia, G. Avoine, *Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags*, International Conference on Smart Card Research and Advanced Applications – CARDIS, volume 3928 of Lecture Notes in Computer Science, pages 289–299, Espagne, 2006.

[CHA2007] F. Chauvet, *Prolongateur d'antenne RFID et système d'échange de données utilisant un tel prolongateur*, brevet FR2896898, CEA, 2007.

[DAN2009] B. Danev, T. S. Heydt-Benjamin, S. Capkun, *Physical-layer Identification of RFID Devices*, 18th USENIX Security Symposium -- USENIX'09, Canada, 2009

[DIM2008] T. Dimitriou, *Proxy Framework for Enhanced RFID Security and Privacy*, Consumer Communications and Networking Conference, 2008.

[DIRFwear] DIFRwear, *DIFRwear's RFID Blocking Products*, http://difrwear.com/.

[DNS2007] DN-Systems, *BBC Reports on Cloning of the new e-passport*, http://www.dnsystems.de/press/document.2007-01-04.2112016470, 2007.

[ECMA340] ECMA-340: *Near Field Communication Interface and Protocol (NFCIP-1)*, ECMA (European Association for Standardizing Information and Communication Systems), Suisse, 2004.

[ECMA352] ECMA-352: *Near Field Communication Interface and Protocol -2 (NFCIP-2)*, ECMA (European Association for Standardizing Information and Communication Systems), Suisse, 2003.

[ECMA356] ECMA-356: *NFCIP-1 - RF Interface Test Methods*, ECMA (European Association for Standardizing Information and Communication Systems), Suisse, 2004.

[ECMA362] ECMA-362: *NFCIP-1 - Protocol Test Methods,* ECMA (European Association for Standardizing Information and Communication Systems), Suisse, 2005.

[ECMA373] ECMA-373: *Near Field Communication Wired Interface (NFC–WI)*, ECMA (European Association for Standardizing Information and Communication Systems), Suisse, 2003.

[EP1650581] S. Ishimura, A. Iketani, *System for determining the position of a relay transponder in order to detect a relay attack on a passive keyless entry system*, 2006.

[FilRFID] FilRFID, Le fil rouge de la RFID, http://www.filrfid.org/.

[FIN2003] K. Finkenzeller, *RFID-Handbook: "Fundamentals and Applications in Contactless Smart Cards and Identification"*, 2003

[FIN2004] T. Finke, H. Kelter.: *Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*. BSI, http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf, Abruf vom 12.10.2004

[FIN2008] D. Finn,., *Smart card with switchable matching antenna*, brevet US0308641, Advanced Microelectronic and Automation Technology Ltd, 2008.

[FOI2004] *Security Aspects and Prospective Applications of RFID Systems*; Federal Office for Information Security, 2004

[FRA2011] A. Francillon, B. Danev, S. Capkun, *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars,* In Proceedings of Network and Distributed System Security Symposium (NDSS), 2011

[GIE2002] T. Giesler, *Chip Card*, brevet US6424029, Koninklijke Philips Electronics N.V, 2002.

[GUE2006] J. Guerrieri, D. Novotny, *HF RFID eavesdropping and jamming test*, Electromagnetics division and Electrical Engineering Laboratory, NIST, 2006.

[HAL2007] M. Halvác, T. Rosa, *A Note on the Relay Attacks on e-Passports: The Case of Czech e-Passports*, Cryptology ePrint Archive, Report 2007/244, 2007.

[HAN2005-A] G. Hancke, *A Practical Relay Attack on ISO 14443 Proximity Cards*, Manuscript, 2005.

[HAN2005-B] G. Hancke, M. Kuhn, *An RFID Distance Bounding Protocol,* In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm, pages 67–73, Grèce, 2005.

[HAN2006] G. Hancke, *Practical Attacks on Proximity Identification Systems* (Short Paper), In IEEE Symposium on Security and Privacy, USA, 2006.

[HAN2007] G. Hancke, *Noisy Carrier Modulation for HF RFID*, In First International EURASIP Workshop on RFID Technology, Autriche, 2007.

[HAN2008-A] G. Hancke, *Eavesdropping Attacks on High-Frequency RFID Tokens*, In Workshop on RFID Security – RFIDSec'08, Hongrie, 2008.

[HAN2008-B] G. Hancke, M. Kuhn, *Attacks on Time-of-Flight Distance Bounding Channels*, In Proceedings of the first ACM Conference on Wireless Network Security, WiSec'08, pages 194–202, USA, 2008.

[HAN2008-C] G. P. Hancke. *Security of Proximity Identification Systems*. Thèse PhD, University of Cambridge, Royaume-Uni, 2008.

[HAN2009] G. Hancke, K. Mayes, K. Markantonakis, *Confidence in Smart Token Proximity: Relay Attacks Revisited*, In Elsevier Computers & Security, 2009.

[HAN2010] G. P. Hancke, *Design of a Secure Distance-Bounding Channel for RFID,* JNCA, 2010.

[HAS2006] E. Haselsteiner, K. Breitfuß, *Security in Near Field Communication Strengths and Weaknesses*, 2006.

[HOS2004] J. HOSHIDA, Article EETimes: *Tests reveal e-passport security flaw*, http://www.eetimes.com/showArticle.jhtml?articleID=45400010, 2004.

[HU2003-A] L. Hu, D. Evans, *Using Directional Antennas to Prevent Wormhole Attacks*, Proceedings of the 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[HU2003-B] Y-C Hu, A. Perrig, D. Johnson, *Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols*, Wise, USA, 2003.

[HU2004] Y. Hu, A. Perrig, and D. Johnson, *Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*, In proceedings of INFOCOM, 2004.

[HU2006] Y.-C. Hu, A. Perrig, D. B. Johnson, *Wormhole Attacks in Wireless Networks*, Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2, pp. 370- 380, 2006.

[IDTECH] Idtechex, *Analyse et recherche dans le domaine de l'électronique imprimée et de la RFID*, http://www.idtechex.com/.

[INS2008] Instructables, *How to block/kill RFID chips*, In: Instructables, http://www.instructables.com/id/How-to-blockkill-RFID-chips/step4/How-to-kill-your-RFID-chip/, 2008.

[ISO10373-6] ISO/IEC 10373-6: *Cartes d'identification -- Méthodes d'essai -- Partie 6: Cartes de proximité*, ISO (International Organization for Standardization), Suisse, 2006.

[ISO10536-1] ISO/IEC 10536-1: *Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes à couplage rapproché -- Partie 1: Caractéristiques physiques*, ISO (International Organization for Standardization), Suisse, 2006.

[ISO10536-2] ISO/IEC 10536-2: *Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Partie 2: Dimensions et emplacement des surfaces de couplage*, ISO (International Organization for Standardization), Suisse, 2006.

[ISO10536-3] ISO/IEC 10536-3: *Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Partie 3: Signaux électroniques et modes de remise à zéro*, ISO (International Organization for Standardization), Suisse, 2006.

[ISO14443-1] ISO/IEC 14443-1: *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics*, ISO (International Organization for Standardization), Suisse, 2008.

[ISO14443-2] ISO/IEC 14443-2: *Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de proximité -- Partie 2: Interface radiofréquence et des signaux de communication*, ISO (International Organization for Standardization), Suisse, 2001.

[ISO14443-3] ISO/IEC 14443-3: *Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de proximité -- Partie 3: Initialisation et anticollision*, ISO (International Organization for Standardization), Suisse, 2001.

[ISO14443-4] ISO/IEC 14443-4: *Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de proximité -- Partie 4: Protocole de transmission*, ISO (International Organization for Standardization), Suisse, 2008.

[ISO15693-1] ISO/IEC 15693-1 : *Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de voisinage -- Partie 1: Caractéristiques physiques*, ISO (International Organization for Standardization), Suisse, 2000.

[ISO15693-2] ISO/IEC 15693-2:*Cartes d'identification -- Cartes à circuit intégré sans contact -- Cartes de voisinage -- Partie 2: Interface et initialisation dans l'air*, ISO (International Organization for Standardization), Suisse, 2006.

[ISO15693-3] ISO/IEC 15693-3:*Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de voisinage -- Partie 3: Anticollision et protocole de transmission,* ISO (International Organization for Standardization) Suisse, 2009.

[ISO18000-3] ISO18000-3 Information technology -- *Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz,* ISO (International Organization for Standardization) Suisse, 2010.

[ISO18092] ISO/IEC 18092: Information technology -- *Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1),* {ISO (International Organization for Standardization), Suisse, 2004.

[JUE2003] A. Juels, R. Pappu, *Squealing Euros: Privacy Protection in RFID-Enabled Banknotes*. In Rebecca N. Wright, editor, Financial Cryptography – FC'03, volume 2742 of Lecture Notes in Computer Science, pages 103–121, Le Gosier, Guadeloupe, French West Indies, January 2003.

[JUE2003] A. Juels, R. Rivest, M. Szydlo, *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*. In Vijay Atluri, editor, Conference on Computer and Communications Security – ACM CCS, pages 103–111, USA, 2003.

[JUE2004] A. Juels, J. Brainard, *Soft Blocking: Flexible Blocker Tags on the Cheap*, Workshop on Privacy in the Electronic Society - WPES, 2004.

[JUE2005] A. Juels, P. Syverson, D. Bailey, *High-Power Proxies for Enhancing RFID Privacy and Utility*, Workshop on Privacy Enhancing Technologies - PET, 2005.

[KAR2005] G. Karjoth, P. Moskowitz, *Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced*. Research Report RC 23710, IBM Research Division, Suisse, 2005.

[KAS2009] T. Kasper, D. Oswald, and C. Paar, *EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment*, 10th International Workshop on Information Security Applications – WISA, 2009.

[KAS2010] K. B. Rasmussen, S. Capkun, *Realization of RF Distance Bounding*, USENIX'10, 2010.

[KFI2005] Z. Kfir, A. Wool, *Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems*, In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm, Grèce, 2005.

[KHA2005] I. Khalil, S. Bagchi, N. B. Shroff, *A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks*, Proceedings of the 2005 International Conference on Dependable Systems and Networks, 2005.

[KIM2006] S.-C. Kim, S.-S. Yeo, S. K. Kim, *MARP: Mobile Agent for RFID Privacy Protection*, International Conference on Smart Card Research and Advanced Applications – CARDIS, Lecture Notes in Computer Science, Espagne, 2006.

[KIM2008] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, O. Pereira, *The Swiss-Knife RFID Distance Bounding Protocol*, International Conference on Information Security and Cryptology – ICISC, volume 5461 of Lecture Notes in Computer Science, pages 98–115, Corée, 2008.

[KIR2006] I. Kirschenbaum, A. Wool, *How to Build a Low-Cost, Extended-Range RFID Skimmer*, Cryptology ePrint Archive, Report 2006/054, 2006.

[KOR2005] T. Korkmaz, *Verifying Physical Presence of Neighbours against Replay-based Attacks in Wireless Ad Hoc Networks*, Information Technology: Coding and Computing 2005, ITCC 2005, International Conference On, 2005.

[LAR1994] A. Larchevesque, M. Gaumet, *Carte électronique comportant un élément fonctionnel activable manuellement*, Solaic société anonyme, brevet FR2728710, 1994.

[LAZ2004] L.Lazos, R. Poovendran, Serloc, *Secure Range-Independent Localization for Wireless Sensor Networks*, Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2004.

[LAZ2005] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, *Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach*, IEEE Communication Society, WCNC, 2005.

[LEH2006] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch, *Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices*, In Ambient Intelligence Developments Conference – AmI.d, France, 2006.

[MAL2010] R. Malherbi Martins, S. Bacquet, J. Reverdy, *Multiple loop against skimming attack*. Proceedings of Fifth International Conference on Systems and Networks Communications (ICSNC), ISBN: 978-1-4244-7789-0, France, 2010.

[MEN1999] A. Menhaj, P. Deloof, J. Assaad, J.-M. Rouvaen, *Des systèmes radars dédiés à l'anticollision*, 1999.

[MIT2010] A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, and J. C. Hernandez-Castro. *Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels*. IEEE Communications Letters, 14(2):121–123, July 2010.

[MobileCloak] MobileCloak, *The off switch for "always on" mobile wireless devices, spychips, toll tags, RFID tags and technologies*, www.mobilecloak.com.

[MUN2006] J. Munilla, A. Ortiz, A. Peinado, Distance Bounding Protocols with Void-Challenges for RFID. In Workshop on RFID Security – RFIDSec'06, Autriche, 2006..

[MUN2008] J. Munilla, A. Peinado, *Distance Bounding Protocols for RFID Enhanced by using Void-Challenges and Analysis in Noisy Channels*, Wireless Communications and Mobile Computing, 8(9):1227–1232, 2008.

[MUN2010] J. Munilla, A. Peinado, *Attacks on a Distance Bounding Protocol.* Elsevier Computer Communications, 33(7):884–889, 2010.

[PAR2001] D. Paret, *Identification radiofréquence et cartes à puce sans contact : Description*, 2001

[PAR2003] D. Paret, *Identification radiofréquence et cartes à puce sans contact : Applications*, 2003

[REI2007] J. Reid, J.M. Gonzalez Neito, T. Tang, and B. Senadji, *Detecting relay attacks with timing based protocols*, Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security – ASIACCS '07, pages 204–213, Singapour, 2007.

[RIE2005-A] M. Rieback, B. Crispo, A. Tanenbaum, *Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags*, In International Workshop on Security Protocols – IWSP'05, Lecture Notes in Computer Science, Angleterre, 2005.

[RIE2005-B] M. Rieback, B. Crispo, A. Tanenbaum, *RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management*, Australasian Conference on Information Security and Privacy – ACISP'05, volume 3574 of Lecture Notes in Computer Science, pages 184–194, Australie, 2005.

[RIE2006] M. Rieback, G. Gaydadjiev, B. Crispo, R. Hofman, A. Tanenbaum, *A Platform for RFID Security and Privacy Administration*, In USENIX/SAGE Large Installation System Administration conference – LISA'06, USA, 2006.

[RIE2008] M. R. Rieback, *Security and Privacy of Radio Frequency Identification,* Thèse PhD, Vrije Universiteit, Hollande, 2008.

[SAB2007] J. Sala Sabate, T. Thomas, *Wideband inductive antenna for contactless communication systems*, Brevet FR2923324, CEA, 2007.

[SAV2007] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, J. Reverdy, *RFID Noisy Reader How to Prevent from Eavesdropping on the Communication?*, Workshop on Cryptographic Hardware and Embedded Systems – CHES, volume 4727 of Lecture Notes in Computer Science, pages 334–345, Autriche, 2007

[SER2002] D. Serbanescu, *Non contact card and reader, two levels of physical security for communication*, EP1256904, 2002

[SIN2007] D. Singelee, B. Preneel, *Distance Bounding in Noisy Environments*, proceeding of the 4th European conference on security and privacy in ad-hoc and sensor networks, 2007.

[TICE] http://tice.utc.fr/moodle/file.php/498/SupportWeb/co/Module_RCSF_35.html

[TU2007] Y.-J. Tu, S. Piramuthu, *RFID Distance Bounding Protocols*, In First International EURASIP Workshop on RFID Technology, Autriche, 2007.

[VER2008] R. Verdult, *Security analysis of RFID tags*, Information Security Group (GSI), UCL, Belgique, 2008

[WAN2004] W. Wang, B. Bhargava, *Visualization of wormholes in sensor networks*, Proceedings of the ACM workshop on Wireless Security, 2004.

[WEI2006] W. Weichao, B. Bharat, Y. Lu, X. Wu, *Defending agains Wormhole Attacks in Mobile Ad Hoc Networks*, Wireless Communication and Mobile Computing, 2006.

[WO0125060] T. Desai, *Relay attack detection of a secure vehicle command communication*, WO0125060, 2001.

[WO114227] K. R. Riemschneider, H. Roehm, M. Wendt, T. Dürbaum, A. Hilgers, R. Pietig, H. Pelzer, *Method and arrangment for increasing the security of tranponders systems, particularly for access to automobiles*, WO114227, 2004.

[WO0255909] F. Pavatich, C. J. Englefield, S. Tsolakis, Security system, US2006/0255909, 2006

[WO200635361] A. S. Leitch, *Electronic communication system in particular access control system for Passive Keyless Entry, as well as method for detecting a relay attack thereon*, WO200635361, 2006.

[YU2006] P. Yu, P. Schaumont, D. Ha, *Securing RFID with Ultra-Wideband Modulation*, Workshop on RFID Security – RFIDSec'06, Autriche, 2006.

[ZAP2005] RFID-Zapper, https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN), 2005.

[ZET2006] K. Zetter, *Hackers Clone E-Passports*, http://www.wired.com/science/discoveries/news/2006/08/71521?currentPage=1, 2006.

GLOSSAIRE

ATQA/ATQB:	Answer To Request, réponses des cartes conformes à la norme ISO14443-A et B
CLn	Cascade Level n
EOF	End Of Frame o
HF:	High Frequency
MISO/SIMO/MOSI/SOMI	Multiple Inputs Single Output/ Single Input Multiple Outputs/ Multiple Outputs Single input/ Single Output Multiple Inputs
NFC:	Near Field Communication
NVB	Number of Valid Bits
OOK	On/Off Keying
REQA/REQB:	REQuest, premières requêtes des cartes conformes à la norme ISO14443-A et B
RF:	RadioFrequency
RFID :	RadioFrequency IDentification
SOF	Start Of Frame
UID	Unique Identier
UWB	Ultra WideBand
FPGA	Field Programmable Gate Array
VHDL	Very high speed integrated circuit Hardware Description Language
VHDR	Very High Data Rate

FIGURES ET TABLEAUX

1. Figures

2. Tableaux

BREVETS, CONFERENCES, PUBLICATIONS

1. Brevets

- « Procédé de sécurisation d'une communication sans fil, dispositif récepteur et système de communication mettant en oeuvre ce procédé », Sana Ben Hamida, Pierre-Henri Thevenon, Jean-Benoît Pierrot, Olivier Savry, Claude Castelluccia
- « Procédé de protection dans une communication radiofréquence sans contact », Pierre-Henri Thevenon, Olivier Savry

2. Conférences

- e-smart, COPRIM: Contactless privacy manager, Louis Goubin, Malika Izabachene, Olivier Lavoisy, Pierre-Henri Thevenon, Vincent Verneuil, 2011
- C&esar, Eavesdropping on RFID devices, François Vacherand, Elisabeth Crochon, François Dehmas, Jacques Reverdy, Olivier Savry, Pierre-Henri Thevenon, 2009
- Softcom, On the Weakness of Contactless System under Relay Attacks, Pierre-Henri Thevenon, Olivier Savry, Smail Tedjini, 2011
- Softcom, Minimization of energy consumption in passive HF contactless and RFID systems, Pierre-Henri Thevenon, Olivier Savry, Smail Tedjini, 2011
- SPECS (Workshop on security and Privacy for embedded devices in Critical Systems) RFID Security, Pierre-Henri Thevenon, Olivier Savry, Alain Merle, Ricardo Malherbi-Martins, 2011

3. Publications

- Chapitre: Attacks on the physical layer of contactless and RFID systems, Pierre-Henri Thevenon, Ricardo Malherbi-Martins, Olivier Savry, Smail Tedjini, Intech, Current trends and challenges in RFID, ISBN: 978-953-307-356-9, 2011

ANNEXES

1. Antennes

A. Antenne double-huit

Cette antenne a été présentée dans le chapitre « Etat de l'art ».

B. Antenne marguerite

L'antenne marguerite a été développée dans le cadre d'un DRT par Judit Sala Sabate (figure Annexes-1) [SAB2007]. L'objectif est l'étude d'antenne inductive multi-circuits résonants pour les systèmes d'identification sans contact très haut débit. En effet, le débit de transfert de données des lecteurs sans contacts est limité par la bande passante de leurs antennes. Il a donc été nécessaire de développer une nouvelle structure d'antenne permettant des débits très élevés.

L'idée principale est une structure d'antenne à plusieurs circuits résonants accordés à des fréquences identiques produisant un champ coopératif. Le couplage entre les différents circuits inductifs doit être nul car les deux antennes ne doivent pas se perturber pour obtenir une addition constructive des deux champs radiofréquences.

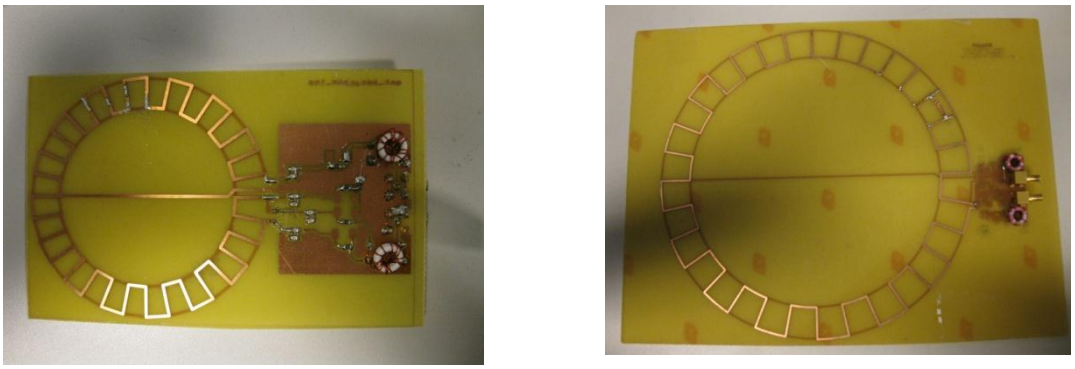


Figure Annexes-1 – Exemples d'antennes marguerites

C. Antenne double boucle

L'antenne double boucle a été développée par Thierry Thomas, ingénieur chercheur au CEA Léti (figure Annexes-2). Cette antenne est constituée d'une paire de boucles dont la géométrie et l'arrangement entre elles permettent d'obtenir un couplage nul entre les deux boucles inductives. Dans cette thèse, cette sonde a été principalement utilisée pour caractériser les différentes antennes que nous avons réalisées. Il est ainsi possible de mesurer la fréquence de résonance d'une antenne et son facteur de qualité. Pour cela, on utilise un analyseur de réseaux en mode « transmission » et on relie l'antenne double boucle aux deux ports ; l'antenne à tester est fermée par une impédance 50Ω et en couplage avec l'antenne double boucle.

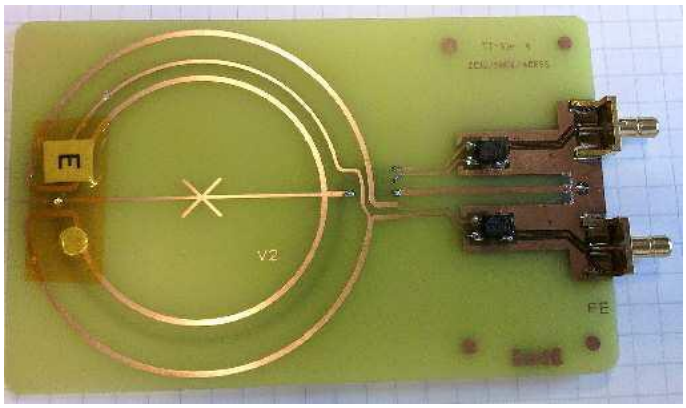


Figure Annexes-2 – L'antenne double boucle

2. Adaptation d'antennes

Il existe de multiples possibilités pour adapter les antennes, nous nous intéressons ici à l'adaptation par pont capacitif et par transformation d'impédance.

A. Adaptation par pont capacitif

La figure Annexes-3 présente le circuit d'adaptation d'un pont capacitif.

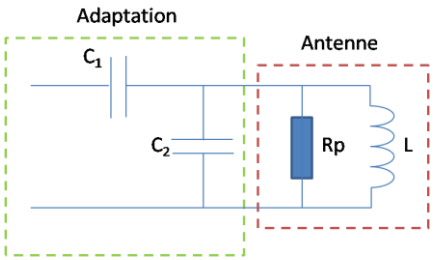


Figure Annexes-3 – Adaptation par pont capacitif

Soit Q le facteur de qualité recherché, la valeur de la résistance série est calculée par l'équation Annexes-1 :

$$R_s = \frac{Lw}{Q} - R_a \qquad \text{(Annexes-1)}$$

On déduit de l'équation Annexes-2 la valeur de la résistance parallèle :

$$R_p = Q^2 (R_a - R_s) \qquad \text{(Annexes-2)}$$

Les équations Annexes-3 et Annexes-4 permettent ensuite de calculer la valeur des deux condensateurs du pont capacitif :

$$C_1 = \frac{1}{w\sqrt{R_c R_p}} \qquad \text{(Annexes-3)}$$

$$C_1 = \frac{1}{Lw^2} \qquad \text{(Annexes-4)}$$

B. Adaptation par transformation d'impédance

La figure Annexes-4 présente le circuit d'adaptation par transformation d'impédance.

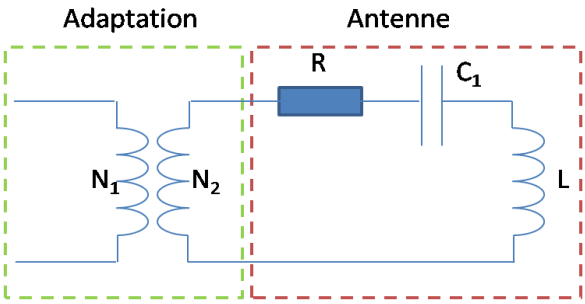


Figure Annexes-4 – Adaptation par transformation d'impédance

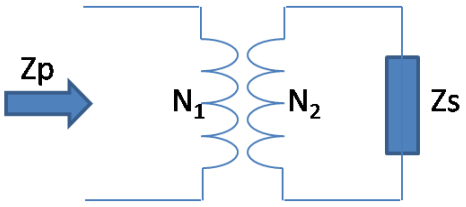


Figure Annexes-5 – Transformation d'impédance

L'équation Annexes-5 donne la valeur du coefficient de qualité en fonction des différents éléments de l'antenne.

$$Q = \frac{1}{R}\sqrt{\frac{L}{C}} \qquad \text{(Annexes-5)}$$

Pour obtenir un grand coefficient de qualité, R doit être petit, du coup on a besoin de réaliser une transformation d'impédance pour obtenir du 50Ω

Soit Q_{voulue} le coefficient de qualité recherché, l'équation Annexes-6 définit la valeur de R en fonction de la valeur du coefficient de qualité recherché.

$$R = \frac{1}{Q_{voulue}}\sqrt{\frac{L}{C}} \qquad \text{(Annexes-6)}$$

La figure Annexes-5montre le schéma d'une transformation d'impédance.

Pour une valeur de Z_p = 50Ω, soit l'impédance voulue de l'antenne, on utilise l'équation Annexes-7 pour trouver la valeur de Z_s

$$Z_s = \frac{1}{Q_{voulue}}\sqrt{\frac{L}{C}}\left(\frac{N_1}{N_2}\right)^2 \qquad \text{(Annexes-7)}$$

Nous avons utilisé l'adaptation par transformation d'impédance pour nos antennes car ce type d'adaptation est plus facile à réaliser et à accorder précisément.

Nous allons détailler les différentes étapes pour accorder et adapter une antenne inductive de type ID1 (format carte sans contact).

L'inductance de l'antenne est généralement connue car elle a été calculée. Elle peut aussi être mesurée en utilisant différents appareils de mesure.

A partir de la valeur de cette inductance, on calcule la valeur du condensateur à mettre en parallèle avec l'inductance de façon à obtenir une fréquence de résonance théorique de 13.56 MHz.

On ajuste ensuite la valeur de ce condensateur en utilisant un analyseur de réseaux et une antenne double boucle. L'analyseur de réseaux affiche la fréquence de résonance. Si elle est trop grande, on augmente la valeur du condensateur

On place ensuite la résistance en série permettant d'avoir le coefficient de qualité souhaité. On utilise alors la règle de transformation d'impédance pour calculer le nombre de spires sur les deux enroulements pour obtenir 50 Ω en entrée de notre antenne. Il est nécessaire de ne pas trop ajouter de spires pour limiter les pertes et afin de pouvoir facilement modifier notre transformateur.

Le circuit réalisé est montré à la figure Annexes-6 :

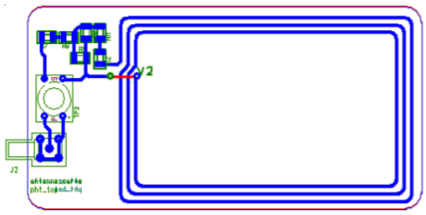


Figure Annexes-6 – Antenne réalisé type ID1

3. Le matériel d'expérimentation

A. Le lecteur sans contact : LRFV7-2

Le lecteur sans contact utilisé pendant cette thèse a été développé par le CEA-Léti. Ces principales caractéristiques sont :

- Conformité
  - ISO 14443-B
  - ISO 14443-A
  - VHDR(Very High Data Rate)
- Débits de transferts très importants
- Modulation de phase et d'amplitude
- Liaison USB et RS232 avec le PC
- Utilisation d'un FPGA

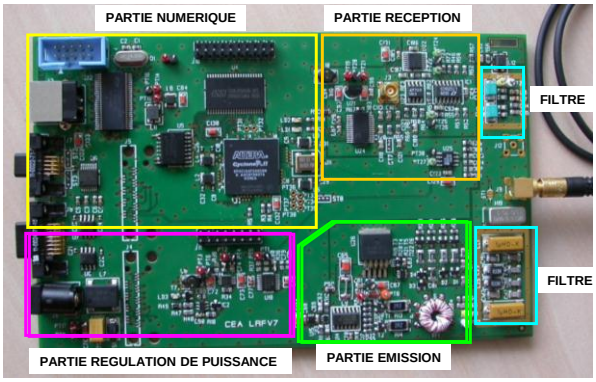


Figure Annexes-7 – Le lecteur Lrfv7

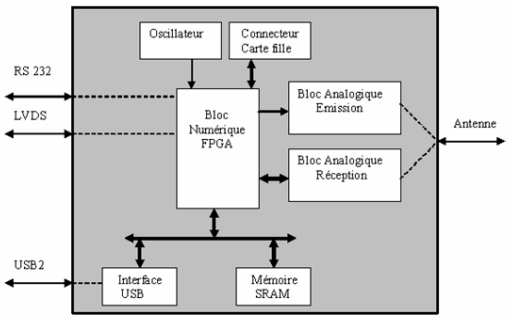


Figure Annexes-8 – Architecture de la carte du Léti

Comme on le voit sur les figures Annexes-7 et Annexes-8 présentant l'architecture de la carte du Léti, celle-ci est constituée de deux blocs analogiques que nous allons présenter.

a. La partie analogique

La partie émission, la partie réception et l'antenne sont toutes connectées aux bornes d'un coupleur directionnel (figure Annexes-9). L'antenne est reliée à l'entrée du composant tandis que les modules analogiques d'émission et de réception sont reliés aux sorties. Ce composant permet de mesurer uniquement la désadaptation de l'antenne lecteur ; c'est-à-dire les variations du couplage entre les antennes lecteur et carte. L'avantage de cette solution est de diminuer l'impact de la porteuse du signal qui a généralement tendance à prendre le dessus sur la modulation de charge de la carte.

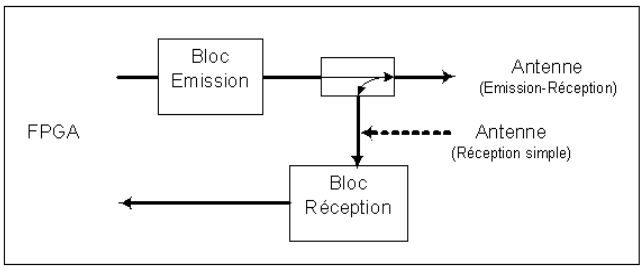


Figure Annexes-9 – Architecture des blocs analogiques

Le module analogique d'émission est constitué de quatre parties

- Un générateur de puissance : Il est possible de générer un signal radiofréquence d'une amplitude suffisante pour alimenter une carte sans contact
- Un filtre passe-bande
- Une alimentation variable : Il est possible de faire varier la puissance du champ radiofréquence émis par le lecteur
- Un modulateur d'amplitude : L'utilisation de transistors permet de moduler la porteuse HF en amplitude

Le modulateur d'amplitude, le générateur de puissance et le filtre se regroupent sur un transformateur torique à trois enroulements (figure Annexes-10).

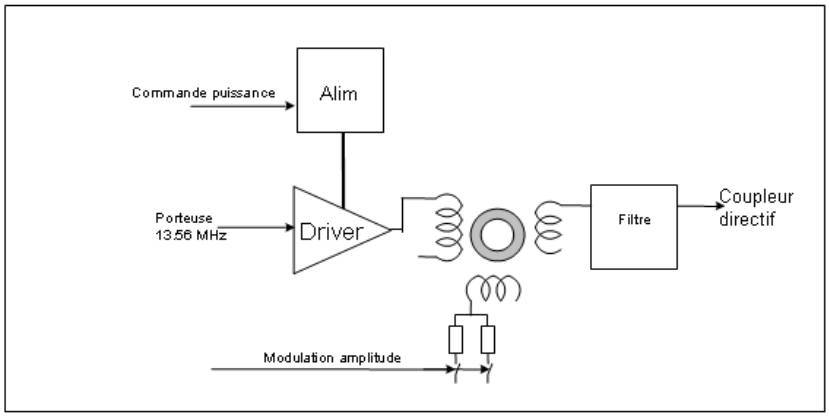


Figure Annexes-10 – Architecture de la partie Emission

Le bloc réception est constitué de (figure Annexes-11):

- Un Filtre Passe-bande
- Un amplificateur avec correcteur automatique de gain : le gain de cet amplificateur est variable et commandé par le FPGA. La correction automatique du gain permet de garder un signal d'amplitude stable en entrée du convertisseur de données ; la résolution des données est alors maximale.
- Un convertisseur analogique numérique : ce composant permet d'échantillonner et de numériser le signal analogique afin de le traiter en VHDL.

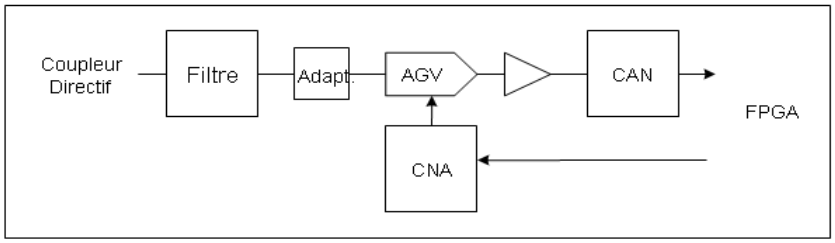


Figure Annexes-11 – Architecture de la partie réception

b. La partie numérique

Tout le bloc numérique est réalisé à partir d'un FPGA Altera.

Nous expliquerons chacune de ces entités VHDL au fur et à mesure de leurs modifications (Annexes-12).

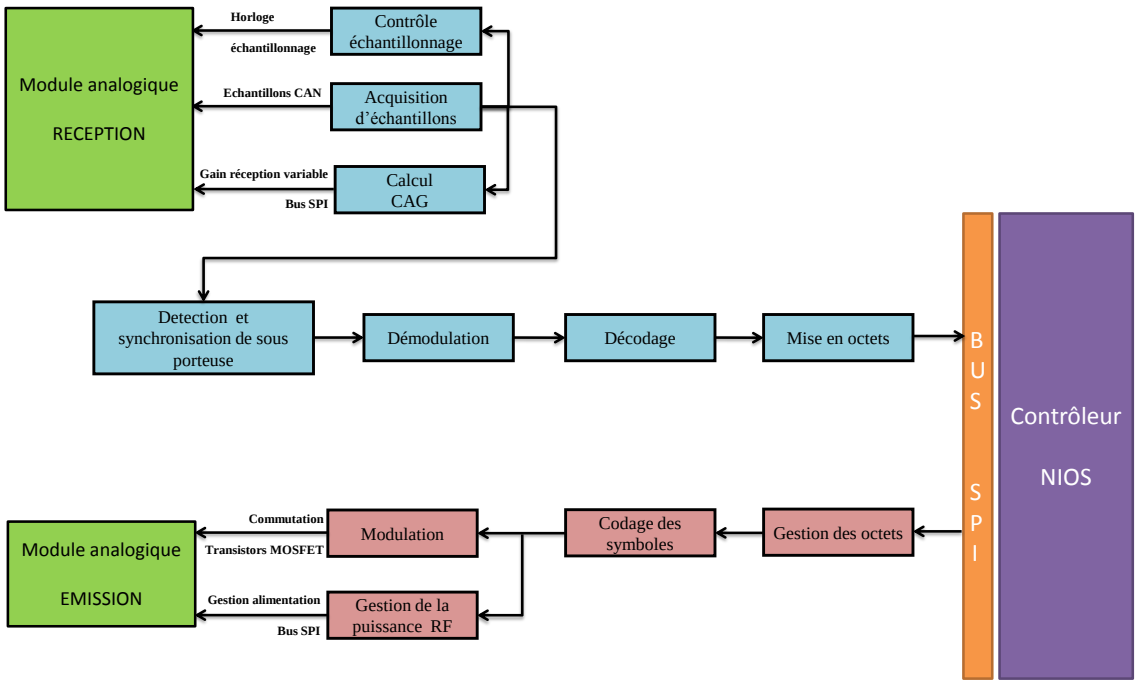


Figure Annexes-12 – L'architecture VHDL du lecteur Lrfv7

c. Le processeur NIOS

Le NIOS est un processeur softcore développé par Altera et qui peut être intégré dans certains de ses FPGA (le Cyclone II par exemple). Un FPGA intégrant un processeur NIOS II combine l'avantage d'être un composant logique programmable et un microprocesseur. Il est donc possible ensuite de créer une interface homme-machine qui interagira en temps réel avec les instructions du processeur.

B. Cartes sans contact de métrologie

a. Carte avec alimentation externe

Cette carte sans contact a été développée au sein du CEA Léti dans le cadre d'un projet européen (figure Annexes-13). La base de cette carte est un ASIC permettant de dépasser le débit binaire de 1 Mbits/s. Cet ASIC est utilisé comme front-end RF de la carte sans contact. Elle permet de démoduler des signaux possédant de 4 à 8 niveaux d'amplitudes différents au lieu de 2 dans les normes actuelles. En effet, cette solution permet en effet d'augmenter le débit sans augmenter la bande passante du système.

La portée maximale de l'ordre de 5 cm. Un FPGA Altera Cyclone permet de traiter les signaux démodulés et de gérer le protocole de communication. La carte est alimentée par une alimentation externe (batterie ou générateur de tension).

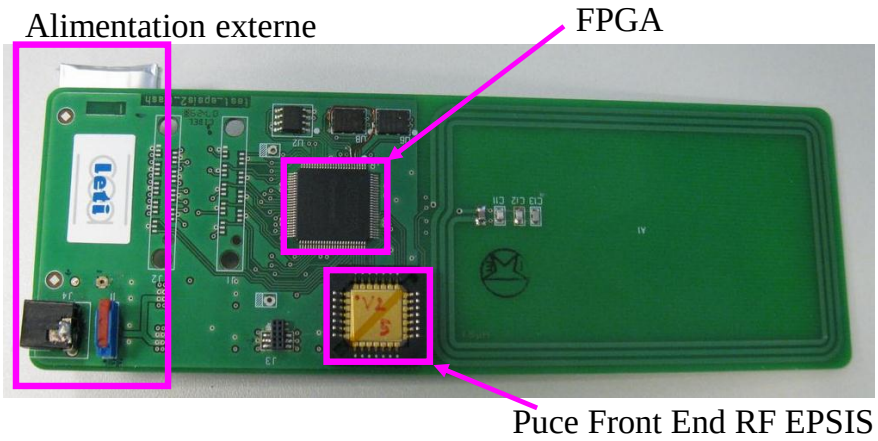


Figure Annexes-13 – La carte de test EPSIS

b. Carte téléalimentée

Le circuit VHDR_FE1 est l'ASIC le plus récent réalisé au sein du CEA ; son objectif est de réaliser une interface sans contact entre un lecteur et une carte téléalimentée. Cette interface analogique numérique est capable de traiter les signaux modulés en phase et en amplitude.

Le circuit VHDR_FE1 est formé de quatre grandes parties distinctes :

- Etages de puissance : Ils redressent, découplent et régulent le signal alternatif issu de l'antenne afin de fournir les tensions d'alimentation du circuit ainsi que deux tensions de service.
- Démodulateur d'amplitude et synchronisation. Le démodulateur d'amplitude fournit un bit d'information selon le niveau d'amplitude du champ magnétique.
- Démodulateur de phase : La mesure de la durée des symboles permet de retrouver les variations de phase qui peuvent valoir jusque de -2π à $+2\pi$.
- Rétro-modulateur. Celui-ci module en charge un seul bit (deux niveaux) en activant ou non un transistor dit de shunt.

La carte de test VHDR est basée sur cet ASIC et sur un FPGA Actel Igloo (figure Annexes-14)

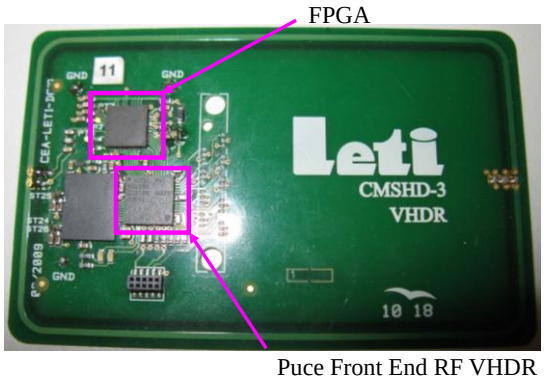


Figure Annexes-14 – La carte de test VHDR

4. Modèles réalisés

A. Fonction de transferts

Les équations Annexes-8 et Annexes-9 correspondent respectivement aux systèmes présentés sur les Annexes-15 et Annexes-16.

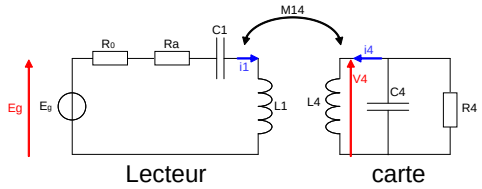


Figure Annexes-15 – Circuit électrique du système sans contact

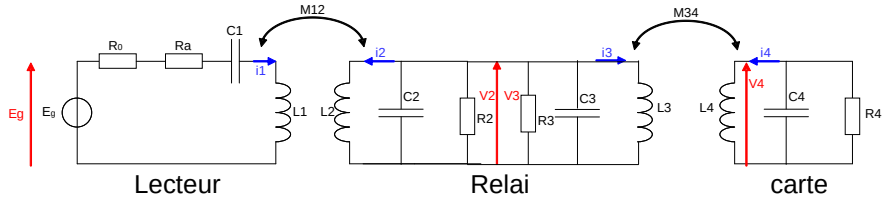


Figure Annexes-16 – Circuit électrique du système sans contact avec relais

$$E_g = \left(R_1 + \frac{1}{jC_1w} + jL_1w\right) I_1 + jM_{14}wI_4$$
$$V_4 = jL_4wI_4 + jM_{14}wI_1$$
$$V_4 = \frac{-R_4}{1 + jR_4C_4w} I_4 \qquad \text{(Annexes-8)}$$

$$E_g = \left(R_1 + \frac{1}{jC_1w} + jL_1w\right) I_1 + jM_{12}wI_2$$
$$V = jL_2wI_2 + jM_{12}wI_1$$
$$V = jL_3wI_3 + jM_{34}wI_4$$
$$V_4 = jL_4wI_4 + jM_{34}wI_3$$
$$V_4 = \frac{-R_4}{1 + jR_4C_4w} I_4 \qquad \text{(Annexes-9)}$$
$$V = (I_2 - I_3)\frac{R_2R_3}{R_3 - R_2 + jR_2R_3C_2w - jR_2R_3C_3w}$$

Les équations Annexes-10 permettent de simplifier l'équation finale:

$$A = R_1 + \frac{1}{jC_1w} + jL_1w$$
$$B = jM_{12}w$$
$$C = jL_2w$$
$$D = jL_3w$$
$$E = jM_{14}w = jM_{34}w \qquad \text{(Annexes-10)}$$
$$F = jL_4w$$
$$G = \frac{R_2R_3}{R_3 - R_2 + jR_2R_3C_2w - jR_2R_3C_3w}$$
$$H = \frac{-R_4}{1 + jR_4C_4w}$$

On obtient finalement dans le cas sans relais, l'équation Annexes-11

$$I_1 = \frac{H - F}{A(H - F) + E^2} \mathrm{E_g} \qquad \text{(Annexes-11)}$$

Dans le cas où l'on place un relais filaire entre le lecteur et la carte sans contact, on obtient l'équation Annexes-12:

$$I_1 = \frac{[A(G - C) + B^2][(D + G)(H - F) + E^2] - G^2(H - F)}{(G - C)[(D + G)(H - F) + E^2] - G^2(H - F)} \mathrm{E_g} \qquad \text{(Annexes-12)}$$

B. Modèles MATLAB

a. Modèle sans contact

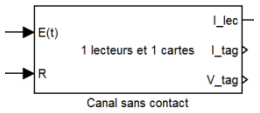


Figure Annexes-17 – Bloc Simulink du modèle sans contact

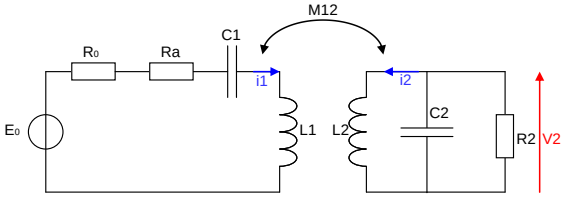


Figure Annexes-18 – Circuit électrique du système sans contact modélisé

Notre système est linéaire à coefficient non constant. Les bibliothèques Simulink ne proposant pas de bloc tout prêt, on le réalise à partir d'une *S-function*.

On se ramène à un système de la forme :

$\begin{cases} \dot{x} = Ax + Bu \\ y = Cx + Du \end{cases}$ où x est le vecteur d'état, u est le vecteur d'entrée, y le vecteur de sortie et A, B, C et D des matrices (à coefficients non constants à priori)

On introduit q_1 la charge du condensateur C_1 : $i_1 = \frac{dq_1}{dt}$

On choisit $y = \begin{bmatrix} i_1 \\ i_2 \\ v_2 \end{bmatrix} x = \begin{bmatrix} q_1 \\ i_1 \\ i_2 \\ v_2 \end{bmatrix}$ et $u = e$

On obtient les équations Annexes-13, Annexes-14, Annexes-15.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ \frac{-L_2}{C_1(L_1L_2 - {M_{12}}^2)} & \frac{-R_1L_2}{L_1L_2 - {M_{12}}^2} & 0 & \frac{-M_{12}}{L_1L_2 - {M_{12}}^2} \\ \frac{M_{12}}{C_1(L_1L_2 - {M_{12}}^2)} & \frac{R_1M_{12}}{L_1L_2 - {M_{12}}^2} & 0 & \frac{1}{L_2} + \frac{{M_{12}}^2}{L_2(L_1L_2 - {M_{12}}^2)} \\ 0 & 0 & \frac{-1}{C_2} & \frac{-1}{R_2C_2} \end{bmatrix} \qquad \text{(Annexes-13)}$$

$$B = \begin{bmatrix} 0 \\ \frac{L_2}{L_1L_2 - {M_{12}}^2} \\ \frac{-M_{12}}{L_1L_2 - {M_{12}}^2} \\ 0 \end{bmatrix} \qquad \text{(Annexes-14)}$$

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \text{(Annexes-15)}$$

b. Relais filaire

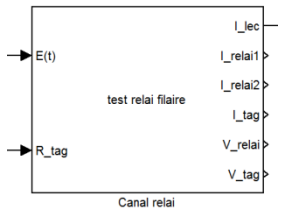


Figure Annexes-19 – Bloc Simulink du relais filaire

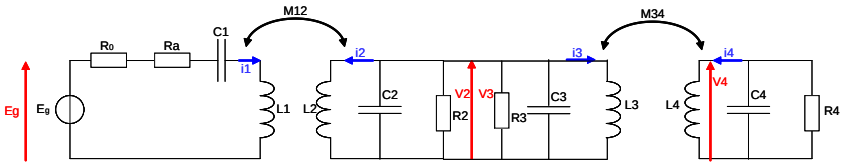


Figure Annexes-20 – Circuit électrique du relais filaire modélisé

On choisit $y = \begin{bmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \\ v \\ v_4 \end{bmatrix}$, $x = \begin{bmatrix} q_1 \\ i_1 \\ i_2 \\ i_3 \\ i_4 \\ v \\ v_4 \end{bmatrix}$ et $u = e$

On trouve les équations Annexes-16, Annexes-17, Annexes-18.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \frac{-L_2}{C_1(L_1L_2 - {M_{12}}^2)} & \frac{-R_1L_2}{L_1L_2 - {M_{12}}^2} & 0 & 0 & 0 & \frac{-M_{12}}{L_1L_2 - {M_{12}}^2} & 0 \\ \frac{M_{12}}{C_1(L_1L_2 - {M_{12}}^2)} & \frac{R_1M_{12}}{L_1L_2 - {M_{12}}^2} & 0 & 0 & 0 & \frac{1}{L_2} + \frac{{M_{12}}^2}{L_2(L_1L_2 - {M_{12}}^2)} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{L_4}{L_3L_4 - {M_{34}}^2} & \frac{-M_{34}}{L_3L_4 - {M_{34}}^2} \\ 0 & 0 & 0 & 0 & 0 & \frac{-{M_{34}}^2L_4}{L_4(L_3L_4 - {M_{34}}^2)} & \frac{1}{L_4} + \frac{{M_{34}}^2}{L_4(L_3L_4 - {M_{34}}^2)} \\ 0 & 0 & 0 & \frac{1}{C_3 - C_3} & 0 & \frac{-1}{R_3(C_2 - C_3)} - \frac{-1}{R_2(C_2 - C_3)} & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{C_4} & 0 & \frac{-1}{R_4C_4} \end{bmatrix} \quad \text{(Annexes-16)}$$

$$B = \begin{bmatrix} 0 \\ \frac{L_2}{L_1L_2 - {M_{12}}^2} \\ \frac{-M_{12}}{L_1L_2 - {M_{12}}^2} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{(Annexes-17)}$$

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{(Annexes-18)}$$

5. Cartes réalisées

A. Relais avec démodulation

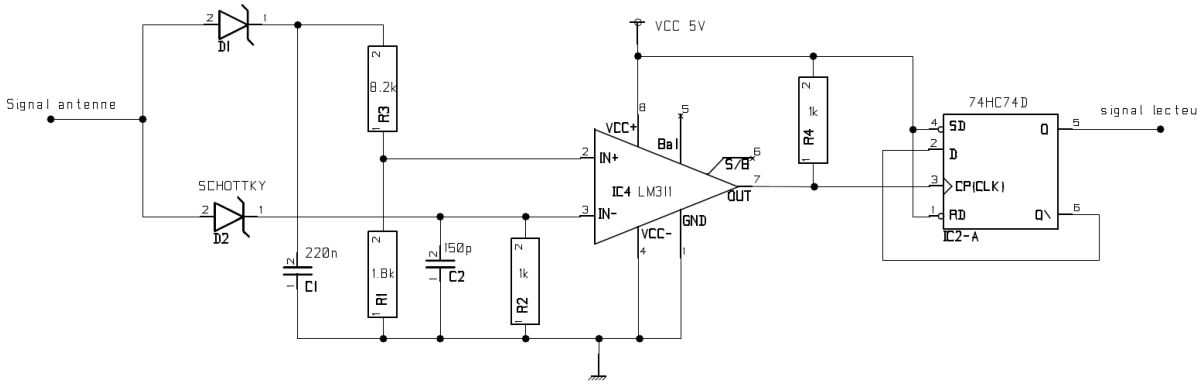


Figure Annexes-21 – Proxy : voie montante

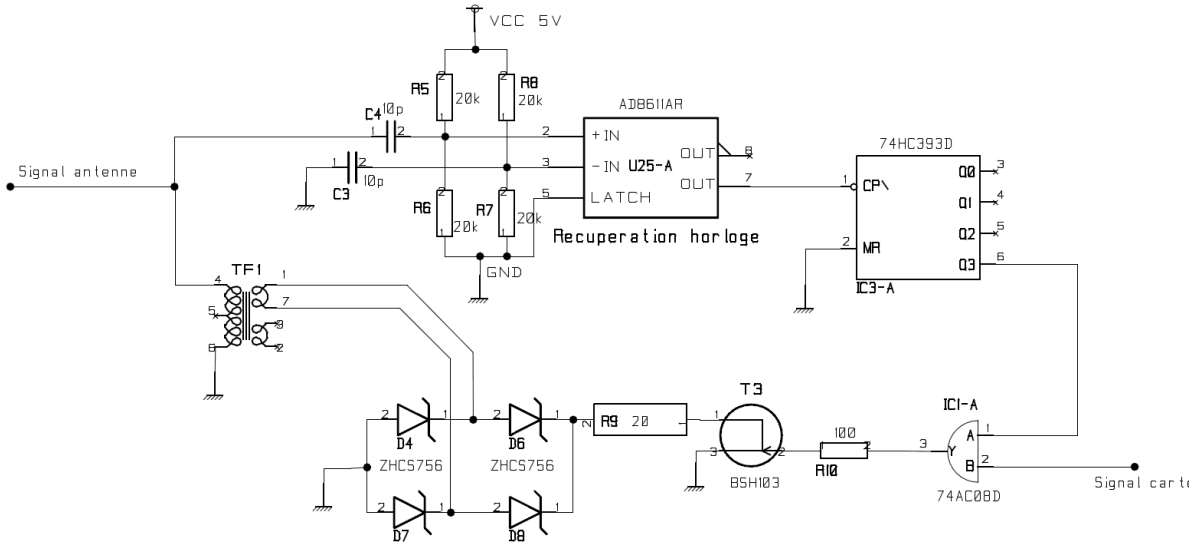


Figure Annexes-22 – Proxy : voie descendante

B. Amplification

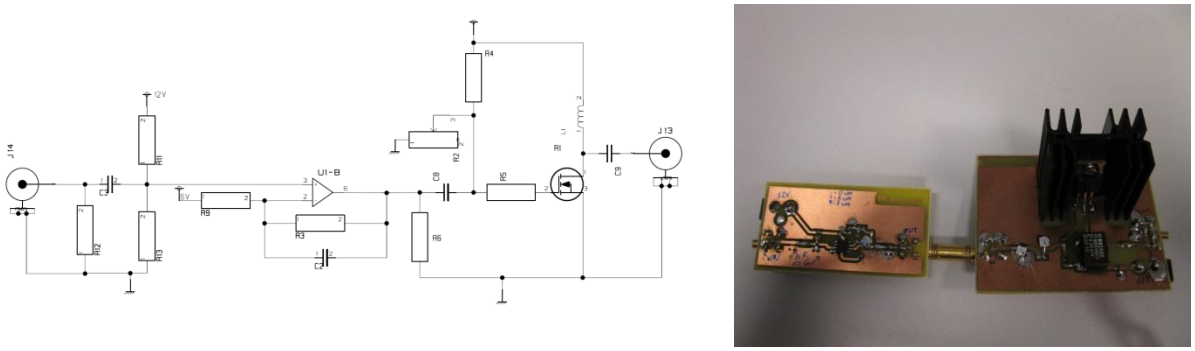


Figure Annexes-23 – Electronique de l'amplification de la voie montante d'un relais

C. Modulation de charge

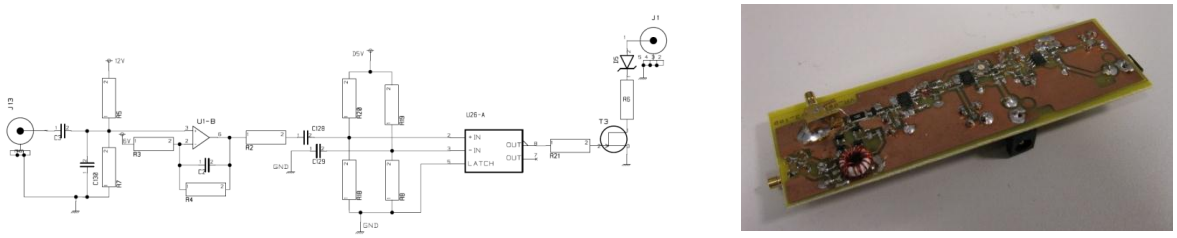


Figure Annexes-24 – Electronique de la voie descendante du relais avec démodulation

D. Carte fille lecteur bruité : modulation d'amplitude

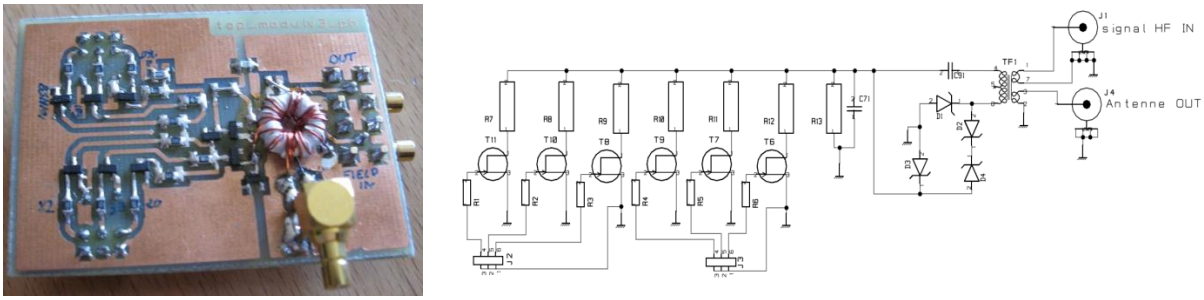


Figure Annexes-25 – Modulation d'amplitude du lecteur

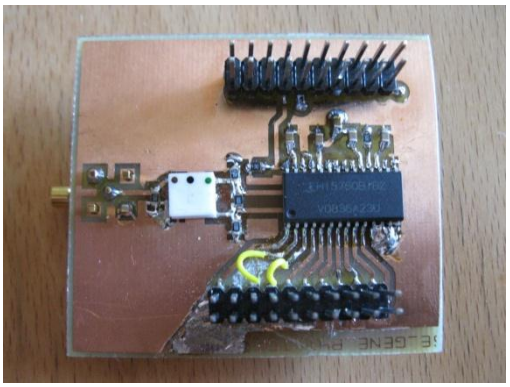


Figure Annexes-26 – Convertisseur numérique-analogique